THEME [SEC-2013.2.5-4]
[Protection systems for utility networks – Capability Project]

Grant agreement for: Collaborative project*

Annex I - "Description of Work"

Project acronym: HYRIM

Project full title: " Hybrid Risk Management for Utility Networks "

Grant agreement no: 608090

Version date: 2014-01-03

Table of Contents

Part A

Workplan Tables

A1:
Project summary

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per project

General information			
Project title [3]	Hybrid Risk Management for Utility Networks		
Starting date [4]	The first day of the month after the signature by the Commission		
Duration in months [5]	36		
Call (part) identifier [6]	FP7-SEC-2013-1		
Activity code(s) most relevant to your topic [7]	SEC-2013.2.5-4: Protection systems for utility networks – Capability Project		
Free keywords [8]		risk management, SCADA, game theory, security,	

Abstract [9]

Risk management is a core duty in critical infrastructures as operated by utility providers. Despite the existence of numerous risk assessment tools to support the utility providers in estimating the nature and impact of possible incidents, risk management up till now is mostly a matter of best practice approaches. Risk management tools are mostly focused on one of two major topics:
- the utility network physical infrastructure, consisting of, e.g. gas, water pipes or power lines
- the utility's control network including SCADA (Supervisory Control and Data Acquisition) networks and business and information systems.

In the context of utility providers, these network types exhibit a significant interaction, and therefore risk management methods that focus on just one of these network types might be insufficient – referred to as interconnected utility infrastructures in this description.
The main objective of this project is to identify and evaluate 'Hybrid Risk Metrics' for assessing and categorising security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms.
The project will provide utility network providers with a risk assessment tool that – in adherence with, e.g., the BSI or ICNC recommendations – supports qualitative risk assessment based on numerical (quantitative) techniques. For that matter, our method will explicitly account for the infrastructure's two-fold nature in terms of the utility network and the control network alongside it. The expected impact is thus a movement away from best practice only, towards the treatment of risk in utility networks based on a sound and well-understood mathematical foundation. The project will take an explicit step towards considering security in the given context of utility networks, ultimately yielding a specially tailored solution that is optimal for the application at hand.

A2:
List of Beneficiaries

Project Number [1]	608090	Project Acronym [2]	HYRIM

List of Beneficiaries

No	Name	Short name	Country	Project entry month[10]	Project exit month
1	AIT Austrian Institute of Technology GmbH	AIT	Austria	1	36
2	Universität Passau	UNI PASSAU	Germany	1	36
3	LANCASTER UNIVERSITY	ULANC	United Kingdom	1	36
4	ETRA INVESTIGACION Y DESARROLLO SA	ETRA	Spain	1	36
5	AKHELA SRL	AKH	Italy	1	36
6	SUMINISTROS ESPECIALES ALGINETENSES COOP. V.	ECA	Spain	1	36
7	LINZ AG FUR ENERGIE, TELEKOMMUNIKATION, VERKEHR UND KOMMUNALE DIENSTE	LINZ AG für Energie,	Austria	1	36

A3:
Budget Breakdown

Project Number [1]	608090	Project Acronym [2]	HYRIM

One Form per Project

Participant number in this project [11]	Participant short name	Fund. % [12]	Ind. costs [13]	Estimated eligible costs (whole duration of the project)					Requested EU contribution
				RTD / Innovation (A)	Demonstration (B)	Management (C)	Other (D)	Total A+B+C+D	
1	AIT	75.0	A	713,760.00	34,106.00	361,016.00	222,740.00	1,331,622.00	1,136,129.00
2	UNI PASSAU	75.0	T	631,208.00	79,998.40	72,365.00	71,313.60	854,885.00	657,082.00
3	ULANC	75.0	T	514,377.60	61,296.00	5,685.00	90,096.00	671,454.60	512,211.00
4	ETRA	50.0	A	485,175.00	155,625.00	2,500.00	131,550.00	774,850.00	454,449.00
5	AKH	50.0	F	257,760.00	149,100.00	18,900.00	57,060.00	482,820.00	279,390.00
6	ECA	75.0	T	113,280.00	148,800.00	0.00	46,080.00	308,160.00	205,440.00
7	LINZ AG für Energie,	50.0	A	117,816.00	65,008.00	0.00	50,972.00	233,796.00	142,384.00
Total				2,833,376.60	693,933.40	460,466.00	669,811.60	4,657,587.60	3,387,085.00

Note that the budget mentioned in this table is the total budget requested by the Beneficiary and associated Third Parties.

*** The following funding schemes are distinguished**

Collaborative Project (if a distinction is made in the call please state which type of Collaborative project is referred to: (i) Small of medium-scale focused research project, (ii) Large-scale integrating project, (iii) Project targeted to special groups such as SMEs and other smaller actors), Network of Excellence, Coordination Action, Support Action.

1. Project number

The project number has been assigned by the Commission as the unique identifier for your project, and it cannot be changed. The project number **should appear on each page of the grant agreement preparation documents** to prevent errors during its handling.

2. Project acronym

Use the project acronym as indicated in the submitted proposal. It cannot be changed, unless agreed during the negotiations. The same acronym **should appear on each page of the grant agreement preparation documents** to prevent errors during its handling.

3. Project title

Use the title (preferably no longer than 200 characters) as indicated in the submitted proposal. Minor corrections are possible if agreed during the preparation of the grant agreement.

4. Starting date

Unless a specific (fixed) starting date is duly justified and agreed upon during the preparation of the Grant Agreement, the project will start on the first day of the month following the entry info force of the Grant Agreement (NB : entry into force = signature by the Commission). Please note that if a fixed starting date is used, you will be required to provide a detailed justification on a separate note.

5. Duration

Insert the duration of the project in full months.

6. Call (part) identifier

The Call (part) identifier is the reference number given in the call or part of the call you were addressing, as indicated in the publication of the call in the Official Journal of the European Union. You have to use the identifier given by the Commission in the letter inviting to prepare the grant agreement.

7. Activity code

Select the activity code from the drop-down menu.

8. Free keywords

Use the free keywords from your original proposal; changes and additions are possible.

9. Abstract

10. The month at which the participant joined the consortium, month 1 marking the start date of the project, and all other start dates being relative to this start date.

11. The number allocated by the Consortium to the participant for this project.

12. Include the funding % for RTD/Innovation – either 50% or 75%

13. Indirect cost model

A: Actual Costs
S: Actual Costs Simplified Method
T: Transitional Flat rate
F :Flat Rate

Workplan Tables

Project number

608090

Project title

HYRIM—Hybrid Risk Management for Utility Networks

Call (part) identifier

FP7-SEC-2013-1

Funding scheme

Collaborative project

WT1
List of work packages

Project Number [1]	608090	Project Acronym [2]	HYRIM

LIST OF WORK PACKAGES (WP)

WP Number [53]	WP Title	Type of activity [54]	Lead beneficiary number [55]	Person-months [56]	Start month [57]	End month [58]
WP 1	Hybrid Risk Metrics and Methodology for Risk Assessment	RTD	1	99.00	1	24
WP 2	Hybrid Risk Assessment for Interconnected Utility Networks	RTD	4	78.00	6	30
WP 3	Human and Organisational Hybrid Risk Analysis	RTD	3	44.00	6	30
WP 4	Perimeter Protection Enhancements	RTD	2	66.00	6	30
WP 5	Evaluation and Assessment of Project Results in Simulated and Real Testbed Environments	DEM	5	72.00	23	36
WP 6	Dissemination, Exploitation and Impact	OTHER	4	50.00	1	36
WP 7	Project Management	MGT	1	31.00	1	36
			Total	440.00		

WT2:
List of Deliverables

Project Number [1]	608090	Project Acronym [2]	HYRIM

List of Deliverables - to be submitted for review to EC

Delive-rable Number [61]	Deliverable Title	WP number [53]	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D1.1	Report on (cyber) risk trends in utility network operator requirements	1	4	51.00	R	CO	12
D1.2	Report on definition and categorisation of Hybrid Risk Metrics	1	1	33.00	R	PU	18
D1.3	Report on categorisation to support standardisation efforts of utilities according to Hybrid Risk Metrics	1	4	15.00	R	PU	24
D2.1	Future trend SCADA-related attack, mitigation and prevention tools	2	4	37.00	R	PU	12
D2.2	Protection and countermeasure policies and processes	2	1	18.00	R	RE	30
D2.3	Software tools for Hybrid Risk Management in SCADA networks	2	5	23.00	P	PU	30
D3.1	Analysis of human and organisational factors in utility vulnerability and resilience	3	3	15.00	R	PP	18
D3.2	Development of a reference architecture with associ-ated metrics and monitoring framework	3	3	7.00	R	PU	30

WT2:
List of Deliverables

Delive-rable Number [61]	Deliverable Title	WP number [53]	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D3.3	Analytical framework and associated metrics	3	3	12.00	P	PP	24
D3.4	Monitoring framework and reference architecture	3	3	10.00	R	PU	30
D4.1	Physical and cyber risk prediction modelling using surveillance systems	4	3	18.00	R	PU	18
D4.2	Guidelines on surveillance technologies to secure utility networks	4	2	15.00	R	PU	24
D4.3	How to enhance perimeter security using new surveil-lance technologies	4	2	33.00	R	PU	30
D5.1	Utility network evaluation guidelines for (cyber) risk investigations	5	5	46.00	R	RE	30
D5.2	Survey regarding consumer and utility provider ac-ceptance	5	6	15.00	R	CO	36
D5.3	Summary of practically applicable results focused on guideline and standardisation for utility providers	5	2	11.00	R	PU	36
D6.1	Dissemination report year 1	6	4	6.00	R	PP	12
D6.2	Dissemination report year 2	6	4	13.25	R	PP	24

WT2:
List of Deliverables

Delive-rable Number [61]	Deliverable Title	WP number [53]	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D6.3	Final dissemination report	6	4	13.75	R	PP	36
D6.4	Exploitation report year 2	6	4	4.25	R	PP	24
D6.5	Final exploitation report	6	4	4.25	R	PP	36
D6.6	Report on standardisation improvement activities	6	4	8.50	R	PP	36
D7.1	Project Handbook	7	1	3.00	R	PP	3
D7.2	Quality Assurance Plan Report	7	5	3.00	R	PP	3
D7.3	Analysis of security-related aspects	7	1	4.00	R	PP	12
D7.4	Management status report 1	7	1	9.00	R	PP	9
D7.5	Management status report 2	7	1	9.00	R	PP	27
D7.6	Ethical Consent and Legal Obligations Report	7	2	1.00	R	PP	6
D7.7	ELAB Status Report	7	2	1.00	R	PP	18
D7.8	ELAB Final Report	7	2	1.00	R	PP	36
			Total	440.00			

WT3:
Work package description

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per Work Package

Work package number [53]	WP1	Type of activity [54]	RTD
Work package title	Hybrid Risk Metrics and Methodology for Risk Assessment		
Start month	1		
End month	24		
Lead beneficiary number [55]	1		

Objectives

- Identification of service parameters in interconnected utility network infrastructures that is sensitive to cyber risks.
- Analysis and modelling of interplay between risks in control networks and utility network infrastructures with focus on cascading effects of failures due to security issues.
- Definition of Hybrid Risk Metrics and Assessment Methods
- Categorisation matrix of utility networks based on:
- utility network type
- threat
- attack impact
- Hybrid Risk Metrics Attributes

Description of work and role of partners

In this work package we focus on the theoretical fundamentals, reused in multiple other parts of the project. We will consider a utility network as a compound of two or more interrelated network infrastructures (control network plus at least one network for (physical) utility delivery) each multiple opportunities of interplay not only for the control network but also between the utility networks. We consider risks and threats applying to multiple levels and aspects. This includes for instance an analysis of how the wider system reacts to a failing utility under consideration of the aggregated user reactions. We will evaluate existing network infrastructures to optimally align theoretical considerations with practical circumstances. Different performance and security measures (failure probability and propagation, degree of resilience to adversarial access, etc.) of the utility network will be considered as individual indicators, yet with an explicit account for their interplay. The resulting risk assessment will thus be a multi-criterion safety and security indicator, i.e., a hybrid risk measure for hybrid risk management/assessment approaches.

Task 1.1 Trend analysis of (cyber) risk on utility networks (AIT, *ULANC*, UNI PASSAU, ETRA, AKH, ECA, LINZ)
We will investigate technological trends bearing the potential to become future threats or also future protective means will be assessed in this task. Also, we consider how the system risks are affected during and after periods where changes to the network are applied. Those changes include technological extensions, updates to hardware and software, but also changes to organisa-tional structures (staff hiring, change of duties, etc.). From this, we will derive future threat scenarios.

Task 1.2 Deriving requirements from utility providers (UNI PASSAU, *ETRA*, AKH, ECA, LINZ)
This task comprises the collection of information about the structure and dynamics (control and response processes) of utility networks. This also includes information about the requirements and use-case surveys elicited from utility providers and interviews on reported safety and security incidents (e.g., cyber-attacks, attacks by insiders, etc.). Using past failures data, dependency and interaction patterns would be extracted using Bayesian inference techniques. Explicit attention will be paid to interaction dynamics among control and utility delivery layers in the network, particularly at interconnection points and components that are highly exposed to or dependent on human operators, including utility provider infrastructure surveys, research of reported incidents, analysis of cascading effects and interplay between risks in control and utility networks.

Task 1.3 Definition of hybrid risk metrics and assessment methods (*AIT*, ULANC, UNI PASSAU, ETRA, AKH)
This task represents an important cornerstone of the project. Motivated by the topology and dynamics data extracted in Task 1.1 and Task 1.2, the interplay between risks in different segments of the system is modelled. A mathematical model is defined and analysed both analytically and then verified using numerical simulation of coupled complex networks. Based on this analysis (equilibrium points, stable regions, initial conditions), the competing processes (e.g. load and capacity growth) are discovered and a static risk measure for each performance indicator is made implicitly (by relying on multi-utility games, i.e. a minimax-approach with optimality understood in Pareto's sense). It is also made explicitly by modelling risk manifestations as stochastic processes and using Bayesian decision theory. While complex networks modelling is explicitly intended to cater for vulnerability propagation and risk manifestation in the network (dynamical aspects of attacks), the game-theory/minimax models will be based on this information to yield the (static snapshot) risk measures for each performance indicator in the current situation. The assessment meth-ods for the risk are arising via the steps undertaken to set up and analyse the respective static and dynamic risk evolution models.

Task 1.4 Categorisation of vulnerabilities based on Hybrid Risk Metrics (UNI PASSAU, *ETRA*, AKH, ECA)
Based on the influence of service parameters and the dynamic threat propagation models developed as part of task 1.3, we will use the risk metrics derived from the static (multi-criteria game) models to classify service parameters in terms of criticality for the infrastructure. The game-theoretic modelling will be an asset in this regard, since the terminology for this classification can be naturally integrated in the game-models. This provides assurance that the criticality classification and the units in which the risk is measured are based on a vocabulary that the utility provider can specify itself, so as to assure communicability and comprehensibility of results.

Person-Months per Participant

Participant number [10]	Participant short name [11]	Person-months per participant
1	AIT	25.00
2	UNI PASSAU	17.00
3	ULANC	12.00
4	ETRA	20.00
5	AKH	9.00
6	ECA	10.00
7	LINZ AG für Energie,	6.00
	Total	99.00

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D1.1	Report on (cyber) risk trends in utility network operator requirements	4	51.00	R	CO	12
D1.2	Report on definition and categorisation of Hybrid Risk Metrics	1	33.00	R	PU	18
D1.3	Report on categorisation to support standardisation efforts of utilities according to Hybrid Risk Metrics	4	15.00	R	PU	24
		Total	99.00			

Description of deliverables

WT3:
Work package description

D1.1) Report on (cyber) risk trends in utility network operator requirements: Our trend analysis will extend state-of-the-art knowledge about threats in utility networks. This report's core information will focus on (future imaginable) threat trends and requirements, use-cases and applications for hybrid risk management. Information contributed by industrial partners regarding structure, control processes, dynamics, organisational aspects, etc. will be strictly anonymized and presented in a generalized (abstracted) fashion. [month 12]

D1.2) Report on definition and categorisation of Hybrid Risk Metrics: Theoretical aspects and results (implicit static interplay and explicit dynamical vulnerability and risk evolution) will be described and published to the scientific community. This includes the definition and analysis (both analytically and then verified using numerical simulation) of coupled complex networks. Additionally, risk measures for each perfomance indicator will be described by game-theory/minimax models. [month 18]

D1.3) Report on categorisation to support standardisation efforts of utilities according to Hybrid Risk Metrics: Report on how service parameters of existing utility network infrastructures are classified in terms of criticality, based on the theoretical framework developed as part of this work - not revealing any confidential information. The report will also include a compilation of theoretical results in a concise manner to optimally support standardisation efforts later in WP5. [month 24]

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead benefi-ciary number	Delivery date from Annex I [60]	Comments
MS1	(Cyber) Risk trends identified	1	8	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS2	SCADA-related attacks characterised	4	12	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS3	Review first reporting period	1	18	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS4	Influences of human ressources and surveillance on Hybrid Risk Metrics identified	2	24	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT3:
Work package description

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per Work Package

Work package number [53]	WP2	Type of activity [54]	RTD
Work package title	Hybrid Risk Assessment for Interconnected Utility Networks		
Start month	6		
End month	30		
Lead beneficiary number [55]	4		

Objectives

- Characterisation of attacks specifically against SCADA networks (e.g. APT, threats due to personal communication devices, threat development over time, etc.)
- Development/application of different approaches for threat analysis (in interconnected net-works) based on Hybrid Risk Metrics
- Development of preventative policies and processes
- Provision of software-aided tools to assess risks of threats

Description of work and role of partners

We will investigate the impact on various metrics using, e.g., a minimax approach (with game theory) and coupled complex networks threat analysis (using Bayesian techniques, and stochastic processes) in SCADA based scenarios. The outcome of this will allow us to formulate policies that will help to prevent new threats exhibiting e.g. Advanced Persistent Threats (APT) or threats via personal communication devices characteristics and attack patterns. Further, tools and methodologies required for the application of these metrics will be developed. We plan to extract defence measures from existing risk assessment approaches and security literature, and to adapt, extend or generalize these to the setting in interdependent utility network infrastructures. Furthermore, it includes an analysis of maintenance and control processes related to the utility network, in order to discover how vulnerabilities (e.g., malicious devices or users) can manifest themselves in the system to cause damage at some later point in time.

Task 2.1 Identification of SCADA-related attack characteristics as wells as mitigation and prevention tools (AIT, ULANC, UNI PASSAU, *ETRA*, AKH, LINZ)
This task covers the identification and detailed analysis of the SCADA-related attack characteristics, based on envisaged future trends. This includes the technical attack aspects of:
- System specific targets
- Threats via personally owned communication devices (or IoT devices)
- Evolution of attacks over time
- Security policy definition in SCADA
- Security baselines
- Logging and methods to avoid repudiation of acts and transactions
- Privacy enhancing or cryptographic techniques to protect sensitive information;

This will allow the categorization and modelling of the cyber-attacks, and will also allow the recognition/prediction of threat trends.
This task also covers the identification and analysis of the Usage of existing technical threat mitigation tools, e.g. Mobile Device Management (MDM) Systems: These risk mitigation efforts can address both infrastructure and application perspectives. This analysis will be also based in previous research projects and others scientific publications.

Task 2.2 Definition of a Hybrid Risk Metric in SCADA attack scenarios (*AIT*, ULANC, ETRA, AKH)
This task will define in detail a Hybrid Risk Metric in SCADA attack scenarios, based on game theory, Bayesian decision theory and stochastic processes, among others, and utilization the instantiation of the meta-metrics developed in the course of WP1 to the specific threats identified in Task 2.1. In this context, realistic cyber-physical models, metrics and data sets from WP1 and Task 2.1 are required in order to model

the SCADA attacks scenarios. On the other hand, Hybrid Risk Metrics need to consider efficiency, reliability, stability, and market performance.

Task 2.3 Provision of tools for Hybrid Risk Management in SCADA networks based on existing methods (AIT, ULANC, ETRA, *AKH*)
Based on the previous tasks, this task will focus on the design and development different tools for Hybrid Risk Management in SCADA networks. Based on the investigation and extensively analysis of the previous tasks about the SCADA attacks, different algorithms, mathematical models, programming libraries, software for assessing cyber risks in SCADA networks will be designed. In order to detect, assess and mitigate attacks on SCADA networks.

Task 2.4 Application of Hybrid Risk Metrics in defence measures such as preventative policies and processes (*ULANC*, ETRA)
This task will define in detail the application of Hybrid Risk Metrics in defence measures, already defined in Task 2.2, These implies the application of centralized, decentralized or combined security enforcing policies and protection systems, and countermeasure processes.

Person-Months per Participant

Participant number [10]	Participant short name [11]	Person-months per participant
1	AIT	20.00
2	UNI PASSAU	7.00
3	ULANC	15.00
4	ETRA	25.00
5	AKH	9.00
7	LINZ AG für Energie,	2.00
	Total	78.00

List of deliverables

Deliverable Number [61]	Deliverable Title	Lead beneficiary number	Estimated indicative person-months	Nature [62]	Dissemination level [63]	Delivery date [64]
D2.1	Future trend SCADA-related attack, mitigation and prevention tools	4	37.00	R	PU	12
D2.2	Protection and countermeasure policies and processes	1	18.00	R	RE	30
D2.3	Software tools for Hybrid Risk Management in SCADA networks	5	23.00	P	PU	30
		Total	78.00			

Description of deliverables

D2.1) Future trend SCADA-related attack, mitigation and prevention tools: Identification and detailed analysis of the SCADA-related attacks as well as mitigation and prevention tools based on previous research projects and scientific publications. Categorization and modelling of cyber-attacks and recognition/prediction of threat trends. Analysis of existing technical threat mitigation tools addressing both infrastructure and application perspectives. [month 12]

D2.2) Protection and countermeasure policies and processes: Design and development of policies and process in order to detect, assess and mitigate attacks on SCADA networks. Definition of a Hybrid Risk Metric in SCADA

attack scenarios, based on game theory, Bayesian decision theory and stochastic processes. Modelling of attack scenarios on SCADA networks based on realistic cyber-physical models, metrics and data sets from WP1 and D2.1. [month 30]

D2.3) Software tools for Hybrid Risk Management in SCADA networks: Design and development of software tools implementing Hybrid Risk Management in SCADA networks including algorithms, mathematical models, programming libraries and software for assessing cyber risks in SCADA networks. Definition of the application of Hybrid Risk Metrics in defence measures, i.e. centralized, decentralized or combined security enforcing policies and protection systems. [month 30]

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead beneficiary number	Delivery date from Annex I [60]	Comments
MS2	SCADA-related attacks characterised	4	12	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS3	Review first reporting period	1	18	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS4	Influences of human ressources and surveillance on Hybrid Risk Metrics identified	2	24	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS5	Reference architecture, analytical framework and metrics defined	5	30	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT3:
Work package description

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per Work Package

Work package number [53]	WP3	Type of activity [54]	RTD
Work package title	Human and Organisational Hybrid Risk Analysis		
Start month	6		
End month	30		
Lead beneficiary number [55]	3		

Objectives

- Investigation of human and organisational factors that creates vulnerabilities and resilience to threats.
- To develop a framework of analysis, sets of metrics and a reference architecture for the mitiga-tion of threats, particularly those involving personal communication devices (and IoT devices) and advanced persistent threats.

Description of work and role of partners

This topic adds to the technical models investigated in WP2 an investigation of corresponding human and organisational models to support the security architecture of a utility network. It consists of 1) empirical work to study the way in which humans and organisations are both sources of vulnerability and sources of resilience, and 2) development work to build appropriate models for analysing and managing threats to networked infrastructures. It will focus on, but not be restricted to, particular sources of threat - such as the use of personal communication devices and APTs. The result will be a hybrid risk analysis platform that 1) combines qualitative and quantitative elements, 2) combines organisational issues within and outside utility organisations, and 3) combines multiple methods of inquiry like ethnography, interviews and secondary data analysis.

Task 3.1 Investigation of organisational factors in utility organisations (AIT, *ULANC*, LINZ)
This will involve two main activities. The first is ethnography of operator practices in utility organisations, especially their use of mobile devices but more widely the vulnerabilities that arise from working conditions, technology affordances and social context. The aim would be to discover the individual and collective mental models of risk and vulnerability held by individuals and groups involved in utility operations. Past work in this area has concentrated on systems in which there is a single dominant technology - neglecting settings in which different kinds of infrastructure like power distribution and telecommunications come together. These are especially problematic because of the weaknesses created by contradictions between the SRA (Safety, Reliability and Availability) model on which industrial control networks are based and the CIA (Confidentiality, Integrity and Availability) model that underpins computer systems. The second activity will be a set of interviews with staff in utility organisations responsible for security, reliability and quality to elicit the weaknesses and vulnerabilities they have observed. This will provide a basis for inferring their mental models of risk and vulnerability, and comparing them with the operators' mental models inferred in part (1). The scope of the interviews will include the interplay between utility organisations and the broader supply chains of which utilities are a part, and through which cascade effects can operate.

Task 3.2 Investigation of incidents using secondary data (*ULANC*, UNI PASSAU, ETRA)
This will involve the collation and analysis of security incidents in utility organisations described in the public domain or open literature. Our aim will be to understand: 1) how organisational aspects create vulnerabilities in the technology - for example how organisations create incentives for individuals to bypass security controls; 2) how organisational aspects can help mitigate vulnerabilities in the technology - for example how social redundancy among people with overlapping responsibilities can identify loopholes in protective devices; 3) how organisational functioning becomes vulnerable to utility failures - both within utility firms and in their supply chains. An important by-product of this activity would be an assessment of existing incident reporting system in place for utility networks (see NIST special publication 800-61, for example).

Task 3.3 Investigation of risk responses in society (*ULANC*, UNI PASSAU, ETRA)
This will involve a risk perception survey of utility consumers, intended to assess how they would perceive threats to a utility and how they would behave in reaction to a crisis in a utility. This would then be a basis for

agent based modelling, intended to identify and characterise emergent phenomena - particularly the way in which responses to degraded, disrupted or dangerous service (for example the loss of electrical power, or contamination of water supplies) either reduces or exacerbates further development of a utility crisis. This modelling will take account of the large body of research on risk perception and emergent social phenomena such as the social amplification of risk and availability cascades.

Task 3.4 Development of analytical framework and metrics (*ULANC*, UNI PASSAU, ETRA)
This will involve the integration of the empirical work into a vulnerability evolution framework. The emphasis will be on understanding how sociotechnical systems change over time, and how this temporal process creates vulnerability. This will include the way vulnerabilities are created by 1) legacy systems and 'reverse salients' in technology, 2) patches and revisions in rules, procedures and social agreements, and 3) 'risk migration', when countermeasures introduce their own sources of vulnerability. The integration of industrial controls and telecommunications - both in terms of the former adopting standardized, open technologies traditionally found in the latter, and in terms of industrial controls being physically connected to the Internet and corporate networks - is a particularly important process that can create potential vulnerabilities. On the basis of this framework, a set of risk metrics will be produced. These metrics will be compared with and mapped to the exist-ing Common Vulnerability Scoring System (CVSS).

Task 3.5 Development of monitoring approaches & reference framework (AIT, ULANC, *ETRA*)
This will involve the development of approaches to assist in the detection, monitoring and evaluation of vulnerability-creating behaviours. This is likely to draw on past work on policy-based anomaly detection, extending it from the detailed analysis of traffic patterns to manifestations of vulnerability that may only be capable of partial automation. The aim will be to create a uniform representation for expressing anomalies at all levels to facilitate either human or algorithmic analysis that can integrate signs of threat across such levels. This will then lead to the development of a general prevention and mitigation architecture. Given the possibility of sophisticated attacks combining technology and ‚social engineering', this is likely to involve mixed modes of protection, including both technical devices and organisational processes. It will involve inspecting and reviewing existing standards such as ISO 27000 (whose primary focus is confidentiality rather than availability), ANSI/ISA-99 and the related IEC 62443 series, national guidelines such as the UK's CPNI Good Practice Guide, and the Common Criteria for Information Technology Security Evaluation, and in particular NISTIR 7176.

Person-Months per Participant

Participant number [10]	Participant short name [11]	Person-months per participant
1	AIT	5.00
2	UNI PASSAU	6.00
3	ULANC	21.00
4	ETRA	10.00
7	LINZ AG für Energie,	2.00
	Total	44.00

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D3.1	Analysis of human and organisational factors in utility vulnerability and resilience	3	15.00	R	PP	18

WT3:
Work package description

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D3.2	Development of a reference architecture with associ-ated metrics and monitoring framework	3	7.00	R	PU	30
D3.3	Analytical framework and associated metrics	3	12.00	P	PP	24
D3.4	Monitoring framework and reference architecture	3	10.00	R	PU	30
		Total	44.00			

Description of deliverables

D3.1) Analysis of human and organisational factors in utility vulnerability and resilience: An account of an ethnography of operator practices and vulnerabilities in utility organizations and a set of interviews with staff responsible for security, reliability and quality to elicit the weaknesses and vulnerabilities they have observed. This includes the collation and analysis of security incidents in utility organisations described in the public domain or open literature. [month 18]

D3.2) Development of a reference architecture with associ-ated metrics and monitoring framework: A risk perception survey of utility consumers, intended to assess how they would perceive threats to a utility and how they would behave in reaction to a crisis in a utility. This would then be a basis for agent based modelling, intended to identify and characterise emergent phenomena. Special focus lies on risk perception and emergent social phenomena such as the social amplification of risk and availability cascades. [month 30]

D3.3) Analytical framework and associated metrics: An account of the integration of the empirical work into a vulnerability evolution framework. The emphasis will be on understanding how sociotechnical systems change over time, and how this temporal process creates vulnerability. On the basis of this framework, a set of risk metrics will be produced. [month 24]

D3.4) Monitoring framework and reference architecture: An account of the development of approaches to assist in the detection, monitoring and evaluation of vulnerability-creating behaviours. Creation of a uniform representation for expressing anomalies at all levels to facilitate either human or algorithmic analysis that can integrate signs of threat across such levels. Development of a general prevention and mitigation architecture [month 30]

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead benefi-ciary number	Delivery date from Annex I [60]	Comments
MS3	Review first reporting period	1	18	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS4	Influences of human ressources and surveillance on Hybrid Risk Metrics identified	2	24	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT3:
Work package description

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead benefi-ciary number	Delivery date from Annex I [60]	Comments
MS5	Reference architecture, analytical framework and metrics defined	5	30	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT3:
Work package description

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per Work Package

Work package number [53]	WP4	Type of activity [54]	RTD
Work package title	Perimeter Protection Enhancements		
Start month	6		
End month	30		
Lead beneficiary number [55]	2		

Objectives

- Enhancing surveillance technologies of the extended perimeter
- Investigating demand surveillance strategies via novel technologies
- Categorising surveillance strategies based on utility network type and hybrid risk metrics
- Providing guidelines to enhance security and safety of the public through utility surveillance

Description of work and role of partners

Traditional surveillance of the extended perimeter includes technologies such as video, audio or biometric monitoring data. We propose to enhance these to automatically capture situations which require alerts to human operators. We will devise methods to dynamically extend the surveillance technologies on demand, via not-yet existing novel approaches, e.g., temporally facilitating personal communication devices of employees, particularly smart phones, and using their embedded sensors as surveillance add-ons.

Task 4.1 Surveillance techn. trend analysis (*ULANC*, UNI PASSAU, ETRA, AKH, LINZ)
This task will provide a detailed overview of the current technological trends and best practices in the surveillance area. Important here is also to identify which surveillance technologies are used in a certain kind of utility network (has to be coordinated with utility network partners). As a result of Task 4.1, the currently available and future surveillance technologies will be comprehensively outlined and a classification in several dimensions, including the usability of individual technologies in certain utility networks, will be given.

Task 4.2 Dealing with threats by surveillance (UNI PASSAU, *AKH*)
The first goal of Task 4.2 is to analyze and classify the possible threats, which have been identified in WP1, to gain an insight on their detectability by surveillance techniques. To do that, the results from WP2 and WP3, which deal with important example scenarios, will be used. The second outcome of Task 4.2 is an analysis on how the implementation of certain surveillance technologies can help to mitigate threats. Here, a detailed classification is necessary to see what kind of threat can be mitigated to which degree using a certain technology. The last goal of Task 4.2 is to identify treats to surveillance technologies themselves. Here, a risk assessment will be done to see what kind of harm can come to a surveillance system during its usage and how these risks and the resulting threats can be effectively countered.

Task 4.3 Application of surveillance to compute Hybrid Risk Metrics (*UNI PASSAU*, ETRA, AKH)
This tasks aims for applying the metrics developed in WP1 to the specific threats identified in Task 4.2. Therefore, the important parameters to measure threats are extracted from Tasks 4.2 and are matched with the capabilities of surveillance technologies reviewed in Task 4.1. Further, an important goal is to investigate the demand for novel surveillance technologies and their effect on Hybrid Risk Metrics. In particular, the possible impact (in both a positive and negative manner) of modern communication devices on surveillance is analyzed.

Task 4.4 Application of Hybrid Risk Metrics and Assessment to support surveillance (AIT, *UNI PASSAU*, ETRA, AKH)
As an application of the methodologies developed in Task 4.3, Task 4.4 aims to detect and to be able to predict risks and attacks against a system, the surveillance has to be analyzed in multiple dimensions: 1) the physical integrity of the system has to be taken into account (important in this respect are technologies such as, e.g., video surveillance); 2) the cyber security of the IT systems must be considered. To be able to not only react but proactively predict risks for systems, health, and environment, Task 4.4 will use modelling techniques based on

the results of WP1, such as, e.g., Markov chains, to gain an insight on how suspicious behaviour in physical and cyber space can develop. By doing so, patterns that lead to risks can be quantitatively predicted based on the surveillance of the current system state.

Task 4.5 On-Demand Surveillance Enhancement (AIT, *UNI PASSAU*, AKH)
In this task, the capability to automatically trigger alerts via novel approaches to detect malicious situations is investigated using existing AIT software libraries. By applying the detection and prediction patterns developed in Task 4.4 on novel approaches to detect malicious situations, the possible enhancements of on-demand surveillance are investigated. In particular, the potential extensions of the surveillance capabilities by utilising temporally, e.g., employee's smart phones (or an-other of smart device in an IoT scenario) as additional sensors for the surveillance infrastructure, are evaluated. Therefore, technical aspects, like integration and interoperability, are researched, as well as legal aspects, such as data protection and accountability. In the legal context, it is also of importance to achieve a deeper insight on the possible privacy impacts of the new surveillance techniques to achieve both user acceptance and legal compliance.

Person-Months per Participant

Participant number [10]	Participant short name [11]	Person-months per participant
1	AIT	6.00
2	UNI PASSAU	35.00
3	ULANC	5.00
5	AKH	18.00
7	LINZ AG für Energie,	2.00
	Total	66.00

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D4.1	Physical and cyber risk prediction modelling using surveillance systems	3	18.00	R	PU	18
D4.2	Guidelines on surveillance technologies to secure utility networks	2	15.00	R	PU	24
D4.3	How to enhance perimeter security using new surveil-lance technologies	2	33.00	R	PU	30
		Total	66.00			

Description of deliverables

D4.1) Physical and cyber risk prediction modelling using surveillance systems: This deliverable will focus on the predictability of both physical and cyber risks and threats by using new modelling techniques and the hybrid risk metrics developed in WP1 in combination with surveillance systems. The expected results here are to find out how to combine and match hybrid risk metrics with surveillance systems to achieve a valid prediction of risks and threats. In detail, this means that both physical as well as cyber threats have to be analyzed to see if and how different surveillance systems, such as various sensor types, visual monitoring, etc. and their combination have an influence on prediction accuracy with hybrid risk metrics. [month 18]

D4.2) Guidelines on surveillance technologies to secure utility networks: Deliverable 4.2's results are achieved in tight cooperation with stakeholders and regulatory support. The expected goals are to build a practical list of

guidelines that can be employed in application scenarios where either an existing surveillance perimeter shall be upgraded with new monitoring technologies or a new surveillance grid is about to be implemented. Here, the guidelines created in this deliverable can be used to enhance the security in an optimal way, based on the results obtained in task 1.1. [month 24]

D4.3) How to enhance perimeter security using new surveil-lance technologies: The result of this deliverable will be a report that explains in detail how new technologies, such as, e.g., sensor networks or mobile networked communication devices can be used to enhance current surveillance technologies. These advice strategies, which will feature both the enhancement of physical risk and threat detection by using environmental monitoring as well as cyber threat detection by using new modelling approaches to detect abnormal user behaviour, will mainly be build from the results in tasks 4.1 and 4.2. [month 30]

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead benefi-ciary number	Delivery date from Annex I [60]	Comments
MS3	Review first reporting period	1	18	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS4	Influences of human ressources and surveillance on Hybrid Risk Metrics identified	2	24	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS5	Reference architecture, analytical framework and metrics defined	5	30	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT3:
Work package description

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per Work Package

Work package number [53]	WP5	Type of activity [54]	DEM
Work package title	Evaluation and Assessment of Project Results in Simulated and Real Testbed Environments		
Start month	23		
End month	36		
Lead beneficiary number [55]	5		

Objectives

- Engaging with utility providers
- Probing public acceptance of suggested measures
- Evaluating developed tools and approaches in realistic testbed environments

Description of work and role of partners

WP5 deals with the validation of the theoretical methodology and to assess the practicality of the hybrid risk metrics and the respective tools in an existing and active utility network under realistic conditions. We will integrate the output from the other research activities and analyse the performance and usefulness at the consumer, supplier and policy maker level, in order to pave the way for legislations based on the method. This will be ensured by involving the requests and the demands for our approach from a stakeholder base which is will be growing over the course of the project. The consortium members that represent end-user views, AKH, LINZ and ECA, will contribute feedback on the implementation of (their) infrastructure in our model to evaluate the project's approach. They will also contribute with interviews and surveys to investigations regarding the human factor in cyber risk scenarios. Besides this, the methodology and systems will be tested in e.g. the village of Alginet, Valencia (Spain), where a realistic testbed environment will be set up.

Task 5.1 Identification and involvement of end-users (ETRA, ECA, *AKH*, LINZ)
Returning to the utility network providers that supplied use-cases and requirements in the course of WP1, this task will reveal the degree to which the developed method suits the needs and helps tackling risk assessment processes. This will also help in creating usage guidelines to ease the application and aid the usage of the method by (independent) users after the project has been completed.

Task 5.2 Definition of use cases (ETRA, ECA, *AKH*)
Three different and specific Use-cases will be defined. The project will identify three dimensions/layers of investigation (SCADA systems, human factor and perimeter protection by surveillance) carried out in WPs 2 (attacks against SCADA networks), 3 (the human factor and organisational structure responsibility) and 4 (surveillance technologies of the extended perimeter). Consequently, we will define use-cases individually for each of the three aforementioned dimensions. Based on these, we will apply the developed methodology in order to assess the extent to which hybrid risk metrics tackle the identified use-cases under real world conditions.

Task 5.3 Surveys with regards to user acceptance (ETRA, *ECA*, ULANC)
For consumers (e.g. domestic home users), a survey will be conducted (with questionnaire and interview) in order to elicit the degree of intelligibility of hybrid risk metrics for home users, and the degree of acceptance as a meaningful risk measure that helps to develop trust in the system.

Task 5.4 Survey with utility providers (ETRA, *ECA*, ULANC, AKH)
This task is complementary to Task 5.3: for the utility providers, we will conduct interviews targeting the experienced usefulness of hybrid risk metrics and risk management. We will elicit and report on applications and provider's evaluations and experiences when testing hybrid risk metrics in their infrastructure.

Task 5.5 Evaluation, preparation and presentation of results for policy and decision makers (ETRA, ECA, *UNI PASSAU*)
Compilation of the results from Tasks 5.3 and 5.4 into a summary report that shows strengths and weaknesses of the developed methodology. To aid further developments and also support legisla-tion in developing legal frameworks and standards that incorporate hybrid risk metrics, the results will be analysed and presented with the focus on:
- Legal aspects
- Technological aspects
- Guidelines for standardisation and on using the proposed reference architectures.

Person-Months per Participant

Participant number [10]	Participant short name [11]	Person-months per participant
1	AIT	2.00
2	UNI PASSAU	7.00
3	ULANC	5.00
4	ETRA	17.00
5	AKH	21.00
6	ECA	14.00
7	LINZ AG für Energie,	6.00
	Total	72.00

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D5.1	Utility network evaluation guidelines for (cyber) risk investigations	5	46.00	R	RE	30
D5.2	Survey regarding consumer and utility provider ac-ceptance	6	15.00	R	CO	36
D5.3	Summary of practically applicable results focused on guideline and standardisation for utility providers	2	11.00	R	PU	36
		Total	72.00			

Description of deliverables

D5.1) Utility network evaluation guidelines for (cyber) risk investigations: The report will detail the validation method of the theoretical methodologies in order to assess the practicalities of the hybrid risk metrics. The report will be composed by usage guidelines to ease the application and aid the usage of the methodology, a detailed description of the differen and specific use cases (Scada systems, human factor and perimeter protection by surveillance) and finally a short desciption of the selected users groups (domestic home users and utility network providers). [month 30]

D5.2) Survey regarding consumer and utility provider ac-ceptance: In the report the results of the questionnaire and interview conducted among consumer and utily providers will be illustrated and commented in order to evalute different aspects as: degree of intelligibility of hybrid risk metrics for home users, degree of acceptance

by the users and by the utilities provider as a meaningful risk measure that helps to develop trust in the system and experienced usability of the proposed methodologies. [month 36]

D5.3) Summary of practically applicable results focused on guideline and standardisation for utility providers: Summary report that presents results and experiences as well as testbed descriptions in an anonymized form, so that the report can be made available to decision makers (from industry as well as from legislator and from standardisation bodies) and future development project groups. The report that will show strenghs and weakness of the developed methodologies with a special focus on legal aspects and technological aspects. Furthermore a guidelines for standardisation and on using the proposed reference architecture will be part of the report. [month 36]

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead benefi-ciary number	Delivery date from Annex I [60]	Comments
MS5	Reference architecture, analytical framework and metrics defined	5	30	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS6	Review second reporting period	1	36	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT3:
Work package description

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per Work Package

Work package number [53]	WP6	Type of activity [54]	OTHER
Work package title	Dissemination, Exploitation and Impact		
Start month	1		
End month	36		
Lead beneficiary number [55]	4		

Objectives

The objectives of this WP can be summarised as follows:
- to prepare a detailed dissemination and promotion plan, to monitor and update
- to launch and maintain the project's website
- to run specific dissemination actions so as to maximise awareness of the project in relevant sectors and the whole EU
- to run general dissemination actions so as to maximise awareness of the project in the se-curity and computing/IT communities
- to interact with and support relevant standards organisations
- to support regulatory efforts and policy makers
- to prepare industrial exploitation of the project results
- to establish a HyRiM Advisory Board and organise workshops with them

Description of work and role of partners

This WP encompasses three key elements of any research project: dissemination, exploitation planning, and impact, being indispensable for raising awareness of the work undertaken, promotion of results achieved, and ensuring their sustainability and further use. The work planned for WP7 will be split into four separate but closely interconnected tasks devoted to management of the Advisory Board (a board of utilities experts and other potential beneficiaries of our research outputs), all dissemination actions - activity planning, website creation and maintenance, development of dissemination materials and means - standardisation and regulation activities (for policy makers), and finally production of deployment and exploitation plans for the project and for individual partners.
HyRiM‘s dissemination, exploitation and impact actions will ensure that the results of the project are spread across a wide range of potential users through channels that will guarantee the maximum possible visibility. An interest group, together with the HyRiM Advisory Board will be created at the start of the project to guarantee that the aims of the project and the outcomes match the ex-pectation of experts in the field.

Task 6.1: Workshops with utility providers and policy makers (*AIT*, AKH, ECA, LINZ)
In this task we will organise three workshops with utility providers, policy makers, and legislation and standardisation bodies to ensure that end-users are actively involved in the project during the project lifetime to provide requirements, assess the impact of the key outcomes, and give relevant feedbacks to refine the project results. The workshops will also be a venue to present and disseminate project results among the key stakeholders. The first two workshops are scheduled to be held at the middle of the project during year 2, when first results are available. The final workshop will be held towards the end of the project to present the final results to a broad community of utility providers, policy makers and standardisation bodies. For these events professional booklets will be produced that will contain summarised research output tailored to suit the above mentioned audience.

Task 6.2: Dissemination Activities (AIT, ULANC, *UNI PASSAU*, AKH, LINZ)
Dissemination is crucial to make the project's achievements, results, and developed knowledge known to a large audience. Dissemination activities can be divided into three groups: 1) Scientific dissemination towards other researchers and research organisations. 2) Dissemination to industry and corporations to provide direct benefit

and transfer into practice. 3) Dissemination to the wider general public to raise awareness of cloud security issues and solutions.
Scientific dissemination includes scholarly publications at international workshops and conferences. Focus is on high quality venues that are internationally visible, for example, IEEE Symposium on Security and Privacy. While conferences and workshops will be targeted during the complete project duration, journals publications are in focus mainly during the last year of the project to present summarized and cross-work package results.
Industrial dissemination will focus on publications and presentations in industry-driven venues, journals, and trade magazines. A workshop with the Advisory Board, industry representatives and policy makers is planned. In the workshop research results will be presented that are of interest to industrial dissemination.
Dissemination to the wider public will be through a project website and newsletter. Additionally, professional information leaflets (booklets, etc.) will be produced as means of informing a wider audience of our research activities and results.

Task 6.3: Liaison, standardisation and regulation activities (AIT, *ETRA*, AKH)
This task involves activities related to communications, cooperation and on-going exchanges with related research efforts, including liaisons with EU-funded research project and networks of excellence, as well as research initiatives going beyond European boundaries (in the USA and Asia in particular). HyRiM will operate in a competitive and fast-paced field with several players working on similar problems, and hence will benefit from adoption of standards – to generate economy of scale and agreement on implementations.
Therefore, the main objective of this task is to promote and coordinate the creation, in a fast, flexible and trend-setting way, of guidelines and standards related to the HyRiM project, through close collaboration between the project technology partners and policy makers.

Task 6.4: Exploitation Plan (ETRA, *AKH*, LINZ)
A major goal of this WP is to provide support for standardisation and policy makers (legislation activities towards regulation of utility provisioning). This task is about compiling the theoretical and practical project results into a concise form suitable for efficient decision making by legislative, standardisation or other regulatory authorities.

Person-Months per Participant

Participant number [10]	Participant short name [11]	Person-months per participant
1	AIT	14.00
2	UNI PASSAU	3.00
3	ULANC	5.00
4	ETRA	14.00
5	AKH	7.00
6	ECA	3.00
7	LINZ AG für Energie,	4.00
	Total	50.00

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D6.1	Dissemination report year 1	4	6.00	R	PP	12
D6.2	Dissemination report year 2	4	13.25	R	PP	24
D6.3	Final dissemination report	4	13.75	R	PP	36
D6.4	Exploitation report year 2	4	4.25	R	PP	24

WT3:
Work package description

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D6.5	Final exploitation report	4	4.25	R	PP	36
D6.6	Report on standardisation improvement activities	4	8.50	R	PP	36
		Total	50.00			

Description of deliverables

D6.1) Dissemination report year 1: The dissemination report delivers the dissemination activities (e.g. web page) completed and under current planning. Further, each dissemination report will list official publications in journals and conferences. Specifically, this deliverables will define the HYRIM consortium dissemination activities in: - The dissemination of the project results in the scientific domain, - The promotion of the project in the industrial world, - The dissemination via centres and networks of excellence. The general dissemination will include the preparation and distribution of project webpage, brochure, poster, newsletter, presentation, etc. The specific scientific strategy dissemination includes the promotion of the project results by means of technological papers in journals and magazines and the presentation of the project in technical workshops and conferences. [month 12]

D6.2) Dissemination report year 2: Focus in the second year report will be on the summary of the first workshop with the utility providers and policy makers, and efforts for popular scientific dissemination. This deliverables will described in addition the dissemination activities of the consortium during the second year of the project, as described in D6.1, focus on the workshop with the utility providers and policy makers. [month 24]

D6.3) Final dissemination report: The final dissemination report will summarize the final research results from the project, as well as the demonstrator, which integrates the results of several work packages. It will also give details on the second workshop with the utility providers and policy makers. This deliverable will include also a multimedia material of the demonstration of the project results on the different test-sites, in order to attract the attention of the general public to promote the project in general media and press. [month 36]

D6.4) Exploitation report year 2: A detailed Exploitation Plan will be defined with the objective of describing the Consortium and partners strategy for exploiting project outputs at the end of year 2. The Plan will: - Exactly identify the services/products or product components that can be derived from the project results as well as their positioning within the partners' product offering. - Better position the services/product or product components that can be derived from the project based on a survey of the market, an evaluation of main competitors and a study of worldwide best practices. Business plans and IPR models to allow effective exploitation of project results will be developed. In detail, the activities for those results that are of commercial interest to the consortium partners will be: - Analysis of competitors (in Europe) and of best practices outside of Europe. - Consortium and individual Partner Exploitation Plans. - Selection of the business models for technology and services. [month 24]

D6.5) Final exploitation report: A detailed Exploitation Plan will be defined with the objective of describing the Consortium and partners strategy for exploiting project outputs at the end of year 3, including updated information D6.4. [month 36]

D6.6) Report on standardisation improvement activities: Description of standardisation improvement activities throughout the project. In this deliverable will identify in detail the standardization bodies where the project results could contribute to the relevant standards. [month 36]

WT3:
Work package description

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead benefi-ciary number	Delivery date from Annex I [60]	Comments
MS2	SCADA-related attacks characterised	4	12	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS3	Review first reporting period	1	18	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS4	Influences of human ressources and surveillance on Hybrid Risk Metrics identified	2	24	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS6	Review second reporting period	1	36	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT3:
Work package description

Project Number [1]	608090	Project Acronym [2]	HYRIM

One form per Work Package

Work package number [53]	WP7	Type of activity [54]	MGT
Work package title	Project Management		
Start month	1		
End month	36		
Lead beneficiary number [55]	1		

Objectives

This work package covers the overall administration and management of the HyRiM project with the following aims:
- to ensure meeting the objectives as defined in the project plan
- to keep the project schedule and to guarantee the execution of the work plan and the achievement of the project goals on time and within budget
- to provide project steering for the internal developments of the HyRiM project
- administration of the contract and project financial management
- facilitate the users' involvement through the Advisory Board in order to obtain their feed-back and redirect the work, if necessary, to guarantee user-driven results
- overall quality assurance
- liaison between EC and partners
- preparation of progress and management reports
- reporting to the EC

Description of work and role of partners

WP7 focuses on the project management to ensure that quality and timely work is carried out at the HyRiM project level. It will provide the central project coordination functions through the organisation of all required Project Steering Committee meetings, in order to facilitate the elaboration and implementation of commonly agreed global strategy, decisions and work plans. WP7 will further manage that all necessary administrative issues interfacing with the European Commission (report-ing, cost statements, etc.) are covered in due time and supervised by all partners.

The scientific coordination of the project is not included in this WP. This WP only covers financial and administrative management/coordination activities. The efforts and costs related to the scientific coordination of the project are not included in this WP and will not be reported as management, but as RTD activities.

Regarding the creation and compilation of the project reports, the FP7 guidelines for Project Reporting will be followed.

Task 7.1 Legal and Financial Management (*AIT*)
This will ensure efficient legal and financial management of HyRiM.
It covers the establishment and maintenance of financial records, the planning and monitoring of expenses, the co-ordination of cost claim submission by the HyRiM participant organisations, preliminary check of individual cost claims against known criteria, preparation of consolidated cost statements following the rules and format of the EC RTD programmes, monitoring and follow-up of payments, and preparation of payment summaries to each participant and global overviews.
This task will prepare periodic financial reports to support the Project Coordinator in the preparation of the Management Reports, financial chapters at HyRiM Management Meetings and Annual Reviews.
This task will also organize all the necessary work and legal issues for contract management in HyRiM. This covers the tracking of the HyRiM contract with the progress in the project to detect inconsistencies or problems, the proposal and preparation of contract amendments when necessary, the monitoring of the application of the Consortium Agreement, and the monitoring and coor-dination of all the actions related with IPR.

Task 7.2 Management of Project Execution (*AIT*, AKH)
This task will carry out the overall project management and execution of the project. It will closely follow the project progress, co-ordinate the quality assurance functions, provide continuous risk assessment and in case of problems, will initiate the required corrective actions in close cooperation with the concerned partners.
The scope of this task can be summarized in the following actions:
- Monitoring the progress of the work and the agreed deadlines and milestones of the time planning.
- Definition and application of the Quality Assurance Plan
- Coordinating and monitoring the work package Leaders' work following the defined task responsibilities.
- Anticipating potential critical situations and proposing solutions.
- Quality control and packaging of the deliverables based on the reports that will be provided as result of the actions.
- Preparing periodic reports.
- Organizing and chairing project meetings with a periodicity of at least six months and whenever necessary.
- Organizing a panel of external experts to carry out internal technical reviews to track the progress of the project.

Task 7.3 Management of Legal, Ethical, Privacy and Policy Issues (UNI PASSAU)
This task will deal with legal, ethical, privacy and policy issues (LEPPI) within the project, including monitoring of and reporting on the project's compliance with European regulations. All activities in this task will be supervised by the Ethics and Legal Advisory Board (ELAB) and coordinated by the LEPPI Officer. More detailed information is provided in Annex A – Legal and Ethical Issues – User Consent, Privacy, Data Protection.

Person-Months per Participant

Participant number [10]	Participant short name [11]	Person-months per participant
1	AIT	25.00
2	UNI PASSAU	3.00
5	AKH	3.00
	Total	31.00

List of deliverables

Delive-rable Number [61]	Deliverable Title	Lead benefi-ciary number	Estimated indicative person-months	Nature [62]	Dissemi-nation level [63]	Delivery date [64]
D7.1	Project Handbook	1	3.00	R	PP	3
D7.2	Quality Assurance Plan Report	5	3.00	R	PP	3
D7.3	Analysis of security-related aspects	1	4.00	R	PP	12
D7.4	Management status report 1	1	9.00	R	PP	9
D7.5	Management status report 2	1	9.00	R	PP	27
D7.6	Ethical Consent and Legal Obligations Report	2	1.00	R	PP	6
D7.7	ELAB Status Report	2	1.00	R	PP	18
D7.8	ELAB Final Report	2	1.00	R	PP	36
		Total	31.00			

Description of deliverables

D7.1) Project Handbook: The reporting procedures, communication policies and set of templates to be used within the project will be included in the project handbook. These include the roles of different actors in the project management, meeting schedules and template agendas for plenary and PSC meetings, templates for technical and administrative reporting. [month 3]

D7.2) Quality Assurance Plan Report: In the quality assurance plan the quality of the documents delivered is ensured. It contains rules and procedures the project will have to follow in order to guarantee the highest possible quality, including process description for revision and re-approval of deliverables as well as identification of non-conformity and proposal of respective corrections. [month 3]

D7.3) Analysis of security-related aspects: This deliverable, produced by the consortium's Security Scrutiny Committee (SCC), will report on security-related aspects resulting from the project's activities. In particular, it will describe potential vulnerabilities and threats with respect to the project's demonstration activities. Furthermore, security guidance will be provided with respect to these vulnerabilities and threats. [month 12]

D7.4) Management status report 1: First management status report, describing the project management and technical activities, including results, problems incurred and the corrective actions taken. Also includes an approximate budget status. [month 9]

D7.5) Management status report 2: Second management status report, describing the project management and technical activities, including results, problems incurred and the corrective actions taken. Also includes an approximate budget status. [month 27]

D7.6) Ethical Consent and Legal Obligations Report: This deliverable provides details of all partner's ethical consent and legal obligations when using human subjects in their research. Further, a report by the ELAB is provided, commenting on whether the procedures are compliant with current EU directives. This report will be sent to DG RTD for ethics audit. [month 6]

D7.7) ELAB Status Report: This deliverable provides a report by the ELAB on the status of the ethical related issues of any research conducted so far. Additionally, the extent to which it meets EU directives on data, privacy and ethical consent is described. [month 18]

D7.8) ELAB Final Report: This deliverable provides a final report by ELAB documenting the ethical issues that have arisen in the project and how they were resolved to ensure compliance with EU directives. [month 36]

Schedule of relevant Milestones

Milestone number [59]	Milestone name	Lead benefi-ciary number	Delivery date from Annex I [60]	Comments
MS3	Review first reporting period	1	18	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS6	Review second reporting period	1	36	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT4:
List of Milestones

Project Number [1]	608090	Project Acronym [2]	HYRIM

List and Schedule of Milestones

Milestone number [59]	Milestone name	WP number [53]	Lead beneficiary number	Delivery date from Annex I [60]	Comments
MS1	(Cyber) Risk trends identified	WP1	1	8	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS2	SCADA-related attacks characterised	WP1, WP2, WP6	4	12	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS3	Review first reporting period	WP1, WP2, WP3, WP4, WP6, WP7	1	18	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS4	Influences of human ressources and surveillance on Hybrid Risk Metrics identified	WP1, WP2, WP3, WP4, WP6	2	24	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS5	Reference architecture, analytical framework and metrics defined	WP2, WP3, WP4, WP5	5	30	Cf. Table 4 (Section 1.3.2) of part B for means of verification
MS6	Review second reporting period	WP5, WP6, WP7	1	36	Cf. Table 4 (Section 1.3.2) of part B for means of verification

WT5:
Tentative schedule of Project Reviews

Project Number [1]	608090	Project Acronym [2]	HYRIM

Tentative schedule of Project Reviews

Review number [65]	Tentative timing	Planned venue of review	Comments, if any
RV 1	18	Brussels	
RV 2	36	Brussels	

WT6:
Project Effort by Beneficiary and Work Package

Project Number [1]	608090	Project Acronym [2]	HYRIM

Indicative efforts (man-months) per Beneficiary per Work Package

Beneficiary number and short-name	WP 1	WP 2	WP 3	WP 4	WP 5	WP 6	WP 7	Total per Beneficiary
1 - AIT	25.00	20.00	5.00	6.00	2.00	14.00	25.00	97.00
2 - UNI PASSAU	17.00	7.00	6.00	35.00	7.00	3.00	3.00	78.00
3 - ULANC	12.00	15.00	21.00	5.00	5.00	5.00	0.00	63.00
4 - ETRA	20.00	25.00	10.00	0.00	17.00	14.00	0.00	86.00
5 - AKH	9.00	9.00	0.00	18.00	21.00	7.00	3.00	67.00
6 - ECA	10.00	0.00	0.00	0.00	14.00	3.00	0.00	27.00
7 - LINZ AG für Energie,	6.00	2.00	2.00	2.00	6.00	4.00	0.00	22.00
Total	99.00	78.00	44.00	66.00	72.00	50.00	31.00	440.00

WT7:
Project Effort by Activity type per Beneficiary

Project Number [1]	608090	Project Acronym [2]	HYRIM

Indicative efforts per Activity Type per Beneficiary

Activity type	Part. 1 AIT	Part. 2 UNI PAS	Part. 3 ULANC	Part. 4 ETRA	Part. 5 AKH	Part. 6 ECA	Part. 7 LINZ AG	Total
1. RTD/Innovation activities								
WP 1	25.00	17.00	12.00	20.00	9.00	10.00	6.00	99.00
WP 2	20.00	7.00	15.00	25.00	9.00	0.00	2.00	78.00
WP 3	5.00	6.00	21.00	10.00	0.00	0.00	2.00	44.00
WP 4	6.00	35.00	5.00	0.00	18.00	0.00	2.00	66.00
Total Research	56.00	65.00	53.00	55.00	36.00	10.00	12.00	287.00
2. Demonstration activities								
WP 5	2.00	7.00	5.00	17.00	21.00	14.00	6.00	72.00
Total Demo	2.00	7.00	5.00	17.00	21.00	14.00	6.00	72.00
3. Consortium Management activities								
WP 7	25.00	3.00	0.00	0.00	3.00	0.00	0.00	31.00
Total Management	25.00	3.00	0.00	0.00	3.00	0.00	0.00	31.00
4. Other activities								
WP 6	14.00	3.00	5.00	14.00	7.00	3.00	4.00	50.00
Total other	14.00	3.00	5.00	14.00	7.00	3.00	4.00	50.00
Total	97.00	78.00	63.00	86.00	67.00	27.00	22.00	440.00

WT8:
Project Effort and costs

Project Number [1]	608090	Project Acronym [2]	HYRIM

Project efforts and costs

Beneficiary number	Beneficiary short name	Estimated eligible costs (whole duration of the project)						Requested EU contribution (€)
		Effort (PM)	Personnel costs (€)	Subcontracting (€)	Other Direct costs (€)	Indirect costs OR lump sum, flat-rate or scale-of-unit (€)	Total costs	
1	AIT	97.00	698,488.00	27,500.00	111,600.00	494,034.00	1,331,622.00	1,136,129.00
2	UNI PASSAU	78.00	468,560.00	15,909.00	55,800.00	314,616.00	854,885.00	657,082.00
3	ULANC	63.00	369,306.00	5,685.00	46,800.00	249,663.60	671,454.60	512,211.00
4	ETRA	86.00	494,500.00	2,500.00	30,600.00	247,250.00	774,850.00	454,449.00
5	AKH	67.00	351,750.00	0.00	50,600.00	80,470.00	482,820.00	279,390.00
6	ECA	27.00	162,000.00	0.00	30,600.00	115,560.00	308,160.00	205,440.00
7	LINZ AG fü	22.00	150,920.00	4,500.00	33,100.00	45,276.00	233,796.00	142,384.00
Total		440.00	2,695,524.00	56,094.00	359,100.00	1,546,869.60	4,657,587.60	3,387,085.00

1. Project number

The project number has been assigned by the Commission as the unique identifier for your project. It cannot be changed. The project number **should appear on each page of the grant agreement preparation documents (part A and part B)** to prevent errors during its handling.

2. Project acronym

Use the project acronym as given in the submitted proposal. It cannot be changed unless agreed so during the negotiations. The same acronym **should appear on each page of the grant agreement preparation documents (part A and part B)** to prevent errors during its handling.

53. Work Package number

Work package number: WP1, WP2, WP3, ..., WPn

54. Type of activity

For all FP7 projects each work package must relate to one (and only one) of the following possible types of activity (only if applicable for the chosen funding scheme – must correspond to the GPF Form Ax.v):

• **RTD/INNO =** Research and technological development including scientific coordination - applicable for Collaborative Projects and Networks of Excellence

• **DEM =** Demonstration - applicable for collaborative projects and Research for the Benefit of Specific Groups

• **MGT =** Management of the consortium - applicable for all funding schemes

• **OTHER =** Other specific activities, applicable for all funding schemes

• **COORD =** Coordination activities – applicable only for CAs

• **SUPP =** Support activities – applicable only for SAs

55. Lead beneficiary number

Number of the beneficiary leading the work in this work package.

56. Person-months per work package

The total number of person-months allocated to each work package.

57. Start month

Relative start date for the work in the specific work packages, month 1 marking the start date of the project, and all other start dates being relative to this start date.

58. End month

Relative end date, month 1 marking the start date of the project, and all end dates being relative to this start date.

59. Milestone number

Milestone number:MS1, MS2, …, MSn

60. Delivery date for Milestone

Month in which the milestone will be achieved. Month 1 marking the start date of the project, and all delivery dates being relative to this start date.

61. Deliverable number

Deliverable numbers in order of delivery dates: D1 – Dn

62. Nature

Please indicate the nature of the deliverable using one of the following codes

R = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

63. Dissemination level

Please indicate the dissemination level using one of the following codes:

• **PU =** Public

• **PP =** Restricted to other programme participants (including the Commission Services)

• **RE =** Restricted to a group specified by the consortium (including the Commission Services)

• **CO =** Confidential, only for members of the consortium (including the Commission Services)

• **Restreint UE =** Classified with the classification level "Restreint UE" according to Commission Decision 2001/844 and amendments

• **Confidentiel UE =** Classified with the mention of the classification level "Confidentiel UE" according to Commission Decision 2001/844 and amendments

• **Secret UE =** Classified with the mention of the classification level "Secret UE" according to Commission Decision 2001/844 and amendments

64. Delivery date for Deliverable

Month in which the deliverables will be available. Month 1 marking the start date of the project, and all delivery dates being relative to this start date

65. Review number

Review number: RV1, RV2, ..., RVn

66. Tentative timing of reviews

Month after which the review will take place. Month 1 marking the start date of the project, and all delivery dates being relative to this start date.

67. Person-months per Deliverable

The total number of person-month allocated to each deliverable.

Proposal full title: Hybrid Risk Management for Utility Networks

Proposal acronym: HyRiM

Type of funding scheme: Collaborative Project (Small or medium-scale focused research project)

Work programme topic addressed:
Topic SEC-2013.2.5-4 Protection systems for utility networks

Name of the coordinating person:
Dr. Stefan Schauer (technical/scientific lead), Dr. Christian Monyk (management lead)

E-Mail: ict-security@ait.ac.at
Phone: +43(0) 0664 825 14 55, +43(0) 0664 815 78 37
Fax: +43(0) 50550 2813

List of participants:

Participant No.	Participant organisation name	Short name	Country
1. (Co-ordinator)	AIT Austrian Institute of Technology GmbH	AIT	Austria
2.	Lancaster University	ULANC	UK
3.	University of Passau	UNI PASSAU	Germany
4.	ETRA	ETRA	Spain
5.	Akhela	AKH	Italy
6.	Electrical Cooperative of Alginet	ECA	Spain
7.	Linz AG	LINZ	Austria

Abstract

Risk management is a core duty in critical infrastructures as operated by utility providers. Despite the existence of numerous risk assessment tools to support the utility providers in estimating the nature and impact of possible incidents, risk management up till now is mostly a matter of best-practice approaches. Risk management tools are mostly focused on one of two major topics:

- the utility's physical network infrastructure, consisting of, e.g. gas pipes, water pipes or power lines
- the utility's control network including SCADA (Supervisory Control and Data Acquisition) networks and business and information systems.

In the context of utility providers, these network types exhibit a significant interaction, and therefore risk management methods that focus on just one of these network types might be insufficient. Such coupled infrastructures are referred to as interconnected utility infrastructures in this description.

The main objective of this project is to identify and evaluate 'Hybrid Risk Metrics' for assessing and categorising security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms.

We are focusing on sensitive service parameters that represent interconnection points between control networks and individual utility networks, via which a security incident in the control network may result in cascading effects in utility networks. Hence we refer to our approach as ***Hybrid Risk Management*** and ***Hybrid Risk Metrics***. The risk measures we envisage developing will support a *quantitative* risk analysis as well as simulation tools for decision makers and security specialists in their evaluation of threats. This is especially significant since the risk measurement can be in *qualitative* terms in order to avoid the illusion of "hard facts" based on subjective numerical risk estimates provided by humans. Because of the difficulties in providing accurate numerical risk estimates, qualitative risk assessment is recommended e.g. by the German BSI. To unify the advantages of quantitative assessment with the ease and efficiency of a qualitative analysis, our framework will support a qualitative assessment with a sound quantitative mathematical underpinning. Furthermore we consider "the human factor" in our investigations. As a result of this, the full sociological and economic effects over the different networks will be well understood. We will evaluate the identified security measures and Hybrid Risk Metrics in use cases in which attacks on the control networks are carried out (e.g. Advanced Persistent Threats - APT). Special attention will also be paid to scenarios in which personally owned digital/communication devices used in business day to day life compromise the security of a utility control network. Another core topic of interest in this investigation is the combination of monitoring and surveillance of the extended perimeter by triggering "on demand" surveillance by monitoring events to provide the foundation for novel surveillance mechanisms. To foster awareness and early stakeholder involvement, we will demonstrate our hybrid risk management approach to a group of utility providers in various fields (power, water, gas, transport, oil, etc.) as well as to other stakeholders. This will be done using both a simulation environment and a testbed infrastructure provided by participating stakeholders.

The project will provide utility network providers with a risk assessment tool that – in adherence with, e.g., the BSI or ICNC recommendations – supports qualitative risk assessment based on numerical (quantitative) techniques. For that matter, our method will explicitly account for the infrastructure's two-fold nature in terms of the utility network and the control network alongside it. Based on this infrastructure model, the manifestation of threats, vulnerabilities, etc. can be simulated to identify optimal protective measures to achieve maximal safety and security with the aid of, e.g., game-theory for min/max approaches or coupled complex network approaches. The expected impact is thus a movement away from best practice only, towards the treatment of risk in utility networks based on a sound and well-understood mathematical foundation. The project will take an explicit step towards considering security in the given context of utility networks, ultimately yielding a specially tailored solution that is optimal for the application at hand.

Table of contents

List of figures

List of tables

List of acronyms

ACM	Association for Computing Machinery
APT	Advanced Persistent Threat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CIA	Confidentiality, Integrity and Availability
CIIP	Critical Information Infrastructure Protection
CP	Consortium Plenary
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System
DEM	Demonstration
DM	Dissemination Manager
DoS	Denial of Service
EC	European Community
EM	Exploitation Manager
ENISA	European Network and Information Security Agency
EP3R	European Public-Private Partnership for resilience
EU	European Union
FMEA	Failure Mode and Effects Analysis
GI	German Informatics Society
HRM	Hybrid Risk Metric
HyRiM	Hybrid Risk Management for Utility Providers
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
IT	Information Technology
LEPPI	Legal, Ethical, Privacy and Policy Issues Officer
MGT	Management
MS	Milestone
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NSTB	National Transportation Safety Board
PC	Project Coordinator
PSC	Project Steering Committee
PUF	Physical Unclonable Function
ROI	Return Of Investment
RTD	Research and technological development
SCADA	Supervisory Control and Data Acquisition
SG	Security Group
SRA	Safety, Reliability and Availability
SQL	Structured Query Language
TL	Task Leader
TM	Technological Manager
VaR	Value at Risk
WL	Work Package Leader
WP	Work Package

1. Scientific and Technical Quality, Relevance to the Topics Addressed by the Call

In the past few decades we have experienced a significantly increased demand on utilities resulting in an increased rate of automation in utility network controls and interconnection, as well as increasing dependencies between various kinds of utility network infrastructures.

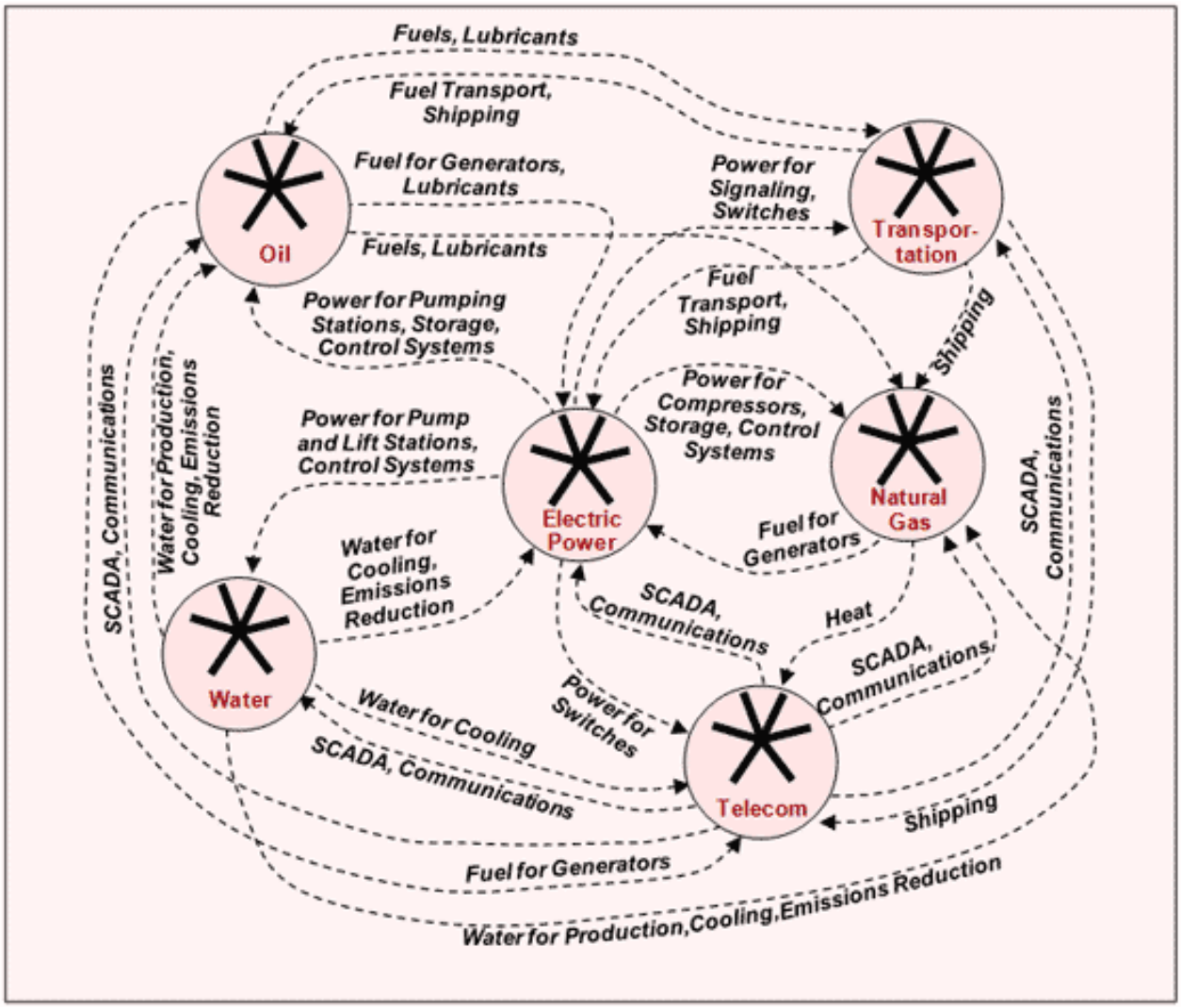

Figure 1: Interdependency between utility infrastructures

Potential failures in utility networks, including those due to cyber-attacks as well as natural disasters, will threaten the fundamental pillars of our modern society. Figure 1 illustrates the potential for cascading effects of the failure of individual utilities[1]. For instance, a scenario in which control systems of a water utility provider are attacked could prove disastrous. To illustrate a simple and well-known, but despite this still effective, attack-example we point to the following: it would be possible for someone without a deep IT security background to look for control network components (e.g. the popular *Simatic* system) via specific search engines (e.g. shodanhq.com) and to access these to tamper with the configuration or to hijack the configuration. Access may be achieved via default user names and passwords or via vulnerabilities of the operating systems of the control units for which numerous exploits exist, especially if they are outdated. Failure due to such an incident in the bespoke water supply can result in reduced availability of water for the cooling of e.g. refineries. This can result in a shortage of gas for heating and for petrol to power our fossil-fuel-driven vehicles.

Due to globalisation and to satisfy the demands of the free market, and to manage the demand at an international level, utilities and their control networks (Supervisory Control and Data Acquisition

[1] Peerenboom Fisher and Whitfield 2001, “Recovering from Disruptions of Interdependent Critical Infrastructures”

– SCADA systems) are being interlinked with those of other, national and international, partners. In the course of this activity, unified EU legislation is ideally needed. In HyRiM we intend to address this issue by supporting the harmonisation of those interlinked control networks, as part of our dissemination activities. Such interlinking of utility infrastructures results in exposing sensitive operational parameters to a multitude of cyber risks. To assess or manage such cyber risks and the interplay between physical risks of failing utilities, best practice methods need to be complemented and superseded by structured risk assessment methodologies in order to categorize and map potential risks that would have adverse effects on the public's safety and security. In order to, e.g., prioritise implementations of costly protection mechanisms or to apply structured risk management approaches, a categorisation of such risk metrics is needed.

1.1. Concept and Objectives

The main objective of this project is to develop and evaluate 'Hybrid Risk Metrics' for assessing and categorising security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms.

We will focus on sensitive service parameters that represent interconnection points between control networks and individual utility networks. A security incident in the control network may result in cascading effects in utility networks via such interconnection points. Hence we refer to risk management spanning over control and utility networks as ***Hybrid Risk Management*** and to related metrics as ***Hybrid Risk Metrics***. The risk measures we envisage developing will support a *quantitative* risk assessment as well as simulation tools to support decision makers and security specialists in their evaluation of threats. This is especially significant since the risk assessment can be in *qualitative* terms in order to avoid the illusion of "hard facts" based on subjective numerical risk estimates provided by humans. Because of the difficulties in providing accurate numerical risk estimates, qualitative risk assessment is recommended (for example) by the German BSI. To unify the advantages of quantitative assessment with the ease and efficiency of a qualitative analysis, our framework will support a qualitative assessment with a sound quantitative mathematical underpinning. Furthermore we consider "the human factor" in our investigations; as a result of this, the full sociological and economic effects over the different networks will be well understood. We will evaluate the identified security measures and Hybrid Risk Metrics in use cases in which attacks on the control networks are carried out (e.g. Advanced Persistent Threats - APT). Special attention will also be paid to scenarios in which personally owned digital/communication devices used in business day to day life compromise the security of a utility control network. Another core topic of interest in this investigation is the combination of monitoring and surveillance of the extended perimeter by triggering "on demand" surveillance by monitoring events. This will provide the foundation for novel surveillance mechanisms which will help to prevent security incidents.

A fundamental objective of HyRiM also is the demonstration and the evaluation of the Hybrid Risk Assessment in a real test bed environment and considering realistic infrastructure configurations in our risk assessment models. The Motivation of for this is to ensure that the research output of this project can be adopted by end-users, i.e. utility providers but also by other stake holders like including legislation, regulation or standardisation bodies – this is important as novel approaches might also require or result in an adaptation of existing regulations and legislation. To achieve this, more than a third of the consortium members represent end-user (utility provider) views. These are Akhela (AKH), Linz AG (LINZ) and The Electrical Cooperative of Alginet (ECA), all together responsible for a mix of utilities involving oil, transportation, sewage, water, gas and electricity. Their requirements and demands will be complemented by a stakeholder base which is initially consisting of a number of other utility providers, and will be growing over the course of the project. They will direct and guide the implementation of (their) infra-structures in our model to evaluate our project's approach.

1.1.1. The Challenge

The challenge in identifying and categorising Hybrid Metrics lies in the variety of (originally) independent utility networks involved and the differences in their scenarios. Additionally, when sensitive

utility network systems are exposed to the Internet it makes them a potential target of new kinds of threats (e.g. Advanced Persistent Threat – APT) which are especially targeted towards SCADA networks. Utility providers may not be aware of the sensitivity of these connections or may underestimate their importance. Hence, the sensitive parameters describing these risks would need to be identified by computer network and security experts in cooperation with domain experts coming from the utility providers. Another challenge for utility providers is the lack of standardisation or regulation resulting in uncertainty about the required investment of computer systems security in utility networks and their control networks. This may lead to an insecure company environment, also including lacking perimeter surveillance, as for instance, malicious software introduced to the network manually via a USB stick dropped in the car park, taken by a curious employee and plugged in into a company laptop, thus infecting the whole system. Such scenarios could be detected by novel surveillance technologies. Another emerging threat is represented by new cultural changes and new business directives such as "bring your own device" (BYOD) or the Internet of Things (IoT), which can result in new attack vectors. Such scenarios result in situations in which mobile computing devices are being used privately and also, for the convenience of their users, to access network services in a utility provider's infrastructure control. All of the above is triggered by human behaviour, i.e. the security awareness (or the lack of it) of a utility provider's employees. Hence, the Human Factor represents another hugely important dimension in our Hybrid Risk Management approach.

1.1.2. Scientific and Technical Objectives

Our first research objective is to develop an identification and characterisation of service parameters which define sensitive interconnection points between control and utility network(s) (**Objective 1**). We subsequently address the following scenarios as mentioned in the call text: i) investigation of scenarios in which attacks are specifically targeted on control networks under consideration of new threats (**Objective 2, 3**) ii) human and organisational risk management (**Objective 4**) and iii) combining risk management with new surveillance methods (**Objective 5**). A final focus of our work is the practical evaluation of all our research activities in a realistic testbed environment (**Objective 6**).

[Objective 1] Definition of hybrid risk metrics and risk assessment processes to enable comprehensive risk management for dealing with threats in multiple (diverse) aspects of utility network infrastructures and to support categorisation of utility infrastructures to prioritise countermeasures development.

Risk assessment is a core duty for operators in multiple utility networks [2,3,4,5,6,7,8]. However, various approaches, mainly based on best practice[9], tend to be used individually for utility control networks

[2] North American Electric Reliability Corporation: *Reliability Standards*, 2012, http://www.nerc.com/page.php?cid=2|20

[3] Matt Luallen: *Securing a Smarter Grid: Risk Management in Power Utility Networks*, SANS Whitepaper 2009, http://www.sans.org

[4] James A. Goodrich and Daniel J. Murray: *Risk Assessment and Management of Water Supply Systems – Infrastructure Initiative for the 21st Century*, 4th U.S. – Japan Governmental Conference on Drinking Water Quality Management and Wastewater Control, January 2007.

[5] *Risk Management of Water Supply and Sanitation Systems*, Proceedings of the NATO Advanced Research Workshop on Risk Management of Water Supply and Sanitation Systems Impaired by Operational Failures Natural Disasters and War Conflicts Ohrid, Macedonia 22-25 October 2008, Springer.

[6] Nesrin Basöz and Anne S. Kiremidjian: *Risk Assessment for Highway Transportation Systems*, Report No. 118, Department of Civil and Environmental Engineering Stanford University, November 1996.

[7] Ziyan Zhao; Jianming Liu; Ruiui Zhang; Kun Lu: *Research of safety and risk assessment technology for power system communication services*, International Conference on Power System Technology (POWERCON), 2010, pp.I-VII, 24-28 Oct. 2010.

and for the utility networks. We are interested in providing and developing sound mathematical foundations to combine and improve the practices in these two areas to capture the interplay between cyber risks and risks to the utility network itself. The core foundation is the definition of Hybrid Risk Metrics for sensitive interconnection points and system parameters. When seeking an accurate model of a utility network, a particular challenge (and obstacle) occurs when the interplay between systems is partially unknown. Utility networks are systems that consist of several interconnected networks that work jointly. While the static structure and dynamics of each individual network may be known, propagation effects of failures or the general interplay may still be difficult to model. This uncertainty will be captured by stochastic and game-theoretic techniques. In particular, the latter has seen elegant applications to network security, with the remarkable feature of the model remaining without needing accurate attacker modelling[10].
Uncertainty in the game-theoretic model itself, however, can be captured by stochastic and Bayesian techniques. Therefore, our proposed method will pursue both approaches to yield an accurate model even without precise or deep insights into a potentially unknown interplay between different layers of the utility network. For the end-user of our research outputs, i.e. utility providers or other stakeholders, the benefit is twofold: variations on the attack scenarios have little influence on the result, so that there is no need to estimate or know the adversary's incentives. On the other hand, the end-user can easily handle uncertainty about the dynamics of the network: where the dynamics are partially known, stochastic techniques can be applied. Where the dynamics are completely unknown, game-theory can help. Using our methodical approach, the investigated scenario will be extendable to the investigation of cascading effects of failures when also considering the interconnection of different utilities with each other. For example, most utility networks depend on a reliable power supply. More importantly, signalling and control of the utility network (e.g. the water supply) may be done via power-line communication, so that with the power supply becoming disrupted, control over possibly more than one other utility network is instantly lost or at least limited. Hybrid risk measures will be designed to let us *a priori* recognize such vulnerabilities, indicated by high risk potential due to widespread implications of a single incident. Our approach will also allow a systematic mapping of properties such as severity of failure and interconnection points to the metrics, which will allow categorisation of the metrics per utility.
The categorization of parameters in terms of their potential impact for safety & security has multiple applications: it provides guidance on where to expect threats and hence facilitates effective safety and security precautions and categorization of threats (in combination with the resulting research outputs satisfying Objectives 2, 3 & 4 for which it is a necessary ingredient in order to develop risk assessment models specific to individual categories of threats).

[Objective 2] Evaluation of hybrid risk metrics for interdependent utility network infrastructures to cope with attacks targeted specifically at utility network controls.

Analysis of the networks current security posture has raised numerous inadequacies, including poor system configuration, poor network security and insufficient software security[11] It is also known that security threats against utility assets have been recognized for decades[12]. In the aftermath of the terrorist attacks on September 11, 2001, great attention has been paid to the security

[8] Xi He, Wei Wang, Xinyu Liu, Yong Ji: R*isk Assessment of Communication Network of Power Company Based on Rough Set Theory and Multiclass SVM*, Physics Procedia, Volume 24, Part B, 2012, pp. 1226-1231.
[9] Guidelines of the German BSI: "IT Grundschutzkatalog Stand 2012"
[10] Tansu Alpcan and Tamer Başar: *Network Security: A Decision and Game Theoretic Approach,* Cambridge University Press, 2010.
[11] National SCADA TestBed (NSTB) Assessments Summary Report: *Common Industrial Control System Cyber Security Weaknesses*, Idaho National Laboratory (INL), May 2010.
[12] *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, McAfee report, 2010

of critical infrastructures. A particular challenge in utility networks arises from their heterogeneous nature, as they are composed of multiple physical networks (at least one utility delivery network on top of which at least one control network is installed). The metrics developed as an output to satisfy Objective 1 will be tested for practicality by an application in a SCADA network. Thus, we pursue a twofold goal: first, we will evaluate the practical feasibility of the developed metrics. Second, we demonstrate how to apply the theoretical framework to a specific class of critical infrastructure. Hybrid risk measures are multi-criteria metrics (vectors) that measure the utility networks performance and attack resilience in terms of several indicators. Therefore, we aim to incorporate models of static parts and the dynamics of their interplay, drawing from Bayesian techniques, stochastic processes, complex coupled networks[13,14,15] threat analysis and game-theory, to derive (pareto-optimal) security strategies[16,17,18.]

We will include a correlation of technical and organisational models to consider the human factor in this scenario. More precisely, we will explicitly study the human factor's degree of impact on the network, e.g. in a case where a member of the administrative team is compromised and mounts an attack from the inside or prepares the ground for a future external adversarial infiltration. This includes vulnerabilities emerging in the network from an attempt to increase the security[19]. The outcome of this will allow us to formulate policies that will help to prevent new threats exhibiting e.g. Advanced Persistent Threats (APT) characteristics and attack patterns. Another primary concern has been the possibility of massive denial of service (DoS) attacks on the SCADA control system and the resulting impacts on the overall performance and stability of the electric power systems. A major objective and challenge here is to keep these policies sufficiently general to apply to a wide range of control (SCADA) networks, but to be specific enough to improve on the existing – mostly conceptual and highly general – literature on risk management. As an equally important output, we seek to gain insight into risk and vulnerability propagation dynamics, so as to be able to identify 'neuralgic' points within the control system of the network. Game-theory essentially deals with optimizations of conflicting goals, such as protective measures and attacks against them. We will go beyond this, by additionally developing models of technological dynamics (of control structures) and social phenomena (e.g., attacks by social engineering via exploiting security "unawareness"), both of which in connection can be turned into a powerful weapon against a utility network (e.g., if the administrative staff, knowing the dynamics of the system can be tricked to release insider knowledge, access codes, etc.). Models that derive a risk metric from the technical properties and the degree of human influence in the system are still missing and are an important goal in this project. Hybrid risk metrics avoid the loss of information or detail that a scalar valued (single) metric would induce, by combining multiple indicators into a measure that reflects both the technological and human risk. Such multi-valued quantitative risk management is missing up till now, and its value or possible improvement over qualitative risk management is very important to investigate.

[13] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, Nat. Phys. 8, 40 (2012)

[14] Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E. & Havlin, S. Catastrophic cascade of failures in interdependent networks. Nature 464, 1025 1028 (2010)

[15] Huang, X., Gao, J., Buldyrev, S. V., Havlin, S. & Stanley, H. E. Robustness of interdependent networks under targeted attack. Phys. Rev. E (R) 83, 065101 (2011).

[16] M. Voorneveld: *Pareto-Optimal Security Strategies as Minimax Strategies of a Standard Matrix Game*, Journal of Optimization Theory and Applications, vol. 102, No. 1, pp. 203-210, (1999).

S. Rass: *On Game-Theoretic Network Security Provisioning,* Springer Journal of Network and Systems Management, (2012)

[17] D. Ghose und U. R. Prasad, *Solution concepts in two-person multicriteria games*, Journal of Optimization Theory and Applications, vol. 63, No. 2, pp. 167-189, (1989)

[18] S. Rass: *On Game-Theoretic Network Security Provisioning,* Springer Journal of Network and Systems Management, (2012)

[19] R.E. Alcock and J.S. Busby: *Risk migration and scientific advance: the case of flame retardant compounds*. Risk Analysis, vol. 26 no. 2, pp. 369-382 (2006).

[Objective 3] Development of tools and methods for risk assessment, which extend existing methodologies towards the handling of new threats (e.g., Advanced Persistent Threats) arising in interconnected utility networks.

Many software platforms used within the different public utilities were developed to operate on legacy systems, which were not designed to be secured from attacks. This software often lacks necessary mechanisms to authenticate all users before allowing system access. Often the systems and protocols used to communicate SCADA traffic lack adequate encryption and authentication. This means that any unauthorized individual which is able to access the physical network layer will be able to perform a man-in-the-middle attack to manipulated valid control functions. These systems also often lack sufficient access control mechanism required to constrain provisioned user privileges and perform auditing of user actions. Although results from research on complex networks have been applied to some limited cases of real-world networks (e.g. world-wide seaport and airport networks[20]), a mathematical framework to study a specific real-world scenario has not been considered yet. Utility networks are often coupled with other utility, control and financial networks, resulting in a system of inter-dependent networks. By applying complex network techniques to study the vulnerability of utility networks, one can provide a quantitative analysis assessing the consequences and risks of targeted attacks and random failures in these networks. Based on the theoretical results coming from Objective 2, we aim to develop methodologies and software tools for risk assessment in interconnected network structures as present within utility providers. Therefore, the mathematical framework developed in Objective 1 and its extension towards SCADA networks will be implemented in a prototype software tool. In the course of this, we plan to extract defence measures from existing risk assessment approaches as well as from current security literature, and to combine it with our newly developed approach. One focus of the risk assessment tools is to model the cascading effects of failures in an interconnected network structure. As already pointed out above, current risk assessment tools are not able to estimate the impact of a failure in one network, for example, the SCADA network, on another computer network, or vice versa. Hence, using current risk assessment methods this impact can only be quantified precisely on one single network and not in its entire significance in the whole interconnected network. Therefore, the mathematical approaches such as game theory and Bayesian techniques developed in Objective 1 are used to tackle this problem in such an interconnected structure. Novel evaluation approaches are required to accurately identify critical vulnerabilities without negatively impacting system operation. The development of improved testing strategies and assessment methodologies must be tailored towards the utilities networks' critical cyber assets, common vulnerabilities, and system availability requirements.

[Objective 4] Definition of security architectures and guidelines to mitigate threats related to human and organisational (including cyber) risk.

This topic deals with the required organisational structures to support the security architecture of a utility network. In particular, the focus lies on the human factor and problems in connection with personal mobile devices, requiring a correlation of technical models with organisational structures. These guidelines will be closely related to e.g. ISO 27001, since the human factor is also a top priority of this standard. We will describe the ethnography of operator practices in utility organisations, with a focus on their use of mobile devices but more widely the vulnerabilities that arise from working conditions, technology 'affordances' and social context. The aim would be to discover the indi-

[20] Parshani, R., Rozenblat, C., Ietri, D., Ducruet, C. & Havlin, S. Inter-similarity between coupled networks. Europhys. Lett. 92, 68002 68006 (2010).

vidual and collective mental models[21] of risk and vulnerability held by individuals and groups involved in utility operations, to discover areas of which they lack awareness, and to explore how effective risk communication processes have been. The most relevant recent scholarship on organisational vulnerability and resilience is the work on 'high reliability organisations' that originated in contexts such as nuclear power generation[22,23], but has been extended into such settings as railroad operations[24] and healthcare[25] - and critical infrastructures in general[26]. But this work concentrates on systems in which there is a single dominant technology - neglecting settings in which, for example, quite different kinds of infrastructure such as power distribution and telecommunications come together. These are especially problematic because - as ENISA (the European Network and Information Security Agency) has observed - typically industrial control networks are built on an SRA (Safety, Reliability and Availability) model whereas IT systems typically use a CIA (Confidentiality, Integrity and Availability) model.

We will further include in our work a set of interviews with staff in utility organisations responsible for security, reliability and quality to elicit weaknesses and vulnerabilities that they have observed. This will provide a basis for inferring the content of their mental models of risk and vulnerability. The scope of the interviews will include not just single utility organisations but the entire utility supply chains of which utilities are a part. This will be rounded up by performing a collation and analysis of security incidents in utility organisations described in the public domain or open literature with the aim to understand three main issues: 1) how organisational aspects create vulnerabilities in the technology - for example how organisations create incentives for individuals to bypass security controls (typically when legitimate actors try to make their day-to-day activities easier or less costly); 2) how organisational aspects can help mitigate vulnerabilities in the technology - for example how social redundancy among people with overlapping responsibilities can identify loopholes in protective devices like authentication mechanisms; 3) how organisational functioning becomes vulnerable to utility failures - and in particular how supply chains both within utilities industries and in consuming industries are threatened by failures and crises in the utility infrastructure. An important by-product of this activity would be an assessment of existing incident reporting system in place for utility networks – see the NIST (the US National Institute of Standards and Technology) special publication 800-61, for example – and a comparison of the taxonomy that emerges from our analysis with published taxonomies used for reporting. This will provide input to an investigation of risk perception based on a survey of utility consumers, intended to assess how they would perceive threats to a utility and how they would behave in reaction to a crisis in a utility. This would then be a basis for agent based modelling taking account of the large body of research on risk perception and emergent social phenomena such as the social amplification of risk and availability cascades.
We will use our results to develop an analytical framework based on Hybrid Risk Metrics which represent a fundamental cornerstone of our investigations, to improve the understanding of how sociotechnical systems change over time, and how this temporal process leads to vulnerabilities. This will include the way vulnerabilities are created by 1) legacy systems and 'reverse salients' in technology, 2) patches and revisions in rules, procedures and social agreements, and 3) 'risk migration', when countermeasures introduce their own sources of vulnerability. The integration of industrial controls and telecommunications - both in terms of the former adopting standardized, open technologies traditionally found in the latter, and in terms of industrial controls being physical-

[21] Morgan, M.G., Fischhoff, B., Bostrom, A. And Atman, C.J, (2001). Risk Communication: A Mental Models Approach. Cambridge University Press

[22] La Porte ,T.R. and Thomas, C.W. 1995. Regulatory compliance and the ethos of quality enhancement: surprises in nuclear power plant operations. Journal of Public Administration Research and Theory, 5: 109-137

[23] Bourrier, M. 1996. Organizing maintenance work as two American nuclear power plants. Journal of Contingencies and Crisis Management, 4: 104-112

[24] Roth, E.M., Multer, J. and Raslear, T. 2006. Shared situation awareness as a contributor to high reliability performance in railroad operations. Organisation Studies, 27: 967-987

[25] Blatt, R., Christianson, M.K., Sutcliffe, K.M. and Rosenthal, M.M. 2006. A sensemaking lens on reliability. Journal of Organisational Behavior, 27: 897-917

[26] Schulman, P., Roe, E., van Eeten, M. and de Bruijne, M. 2004. High reliability and the management of critical infrastructures. Journal of Contingencies and Crisis Management, 12: 14-28

ly connected to the Internet and corporate networks - is a particularly important process that can create potential vulnerabilities. On the basis of this framework, a set of risk metrics will be produced. These metrics will be compared with and mapped to the existing Common Vulnerability Scoring System (CVSS). This will also involve the development of approaches to assist in the detection, monitoring and evaluation of vulnerability-creating behaviours. This is likely to draw on past work on policy-based anomaly detection[27], extending it from the detailed analysis of traffic patterns to manifestations of vulnerability that may only be capable of partial automation.

[Objective 5] Enhancing network and infrastructure surveillance systems using novel, on-demand technologies in the extended perimeter of utility networks.

For a utility provider, both its main facilities and its extended perimeter infrastructure (the latter consisting of assets such as the transportation grid for the provided resources and on-field control system stations) are critical to its business, in order to provide reliable services to its customers. While the core facilities of a utility provider's infrastructure are usually well-equipped with safety-enhancing techniques, such as surveillance technologies, the extended perimeter is often only partly monitored, both in a temporal and local sense. However, there are numerous reasons why surveillance systems in these areas are of special importance. This originates from the highly multi-dimensional risks – such as, e.g., harmful environmental influences or intended, directed attacks that can be either physical or cyber in nature –present in the extended perimeter of a utility provider. In addition, the missing direct supervision of the infrastructure by human operators in combination with the lack of adequate surveillance systems is increasing the potential for harmful influences in the extended perimeter. It is therefore a highly pressing objective to be able to classify the currently used surveillance techniques depending on their technological base, e.g., video surveillance or environmental monitoring by sensors, which in turn enables a more effective use of the currently present, traditional surveillance infrastructure.
Traditional surveillance of the extended perimeter presently includes technologies such as video, audio or biometric monitoring data. While these systems are a sound approach to survey a certain area of the extended perimeter, they have limitations: due to their immobile nature, the systems remain inflexible. Also, the failure of such a system often results in gaps and holes in the surveillance grid, leaving certain parts of the infrastructure without monitoring, as most current surveillance systems do not use self-protection mechanisms. We propose to enhance the present systems to automatically identify system states which require the assistance of human operators in order to mitigate risks more effectively. The approach in this direction is to not only use the current state-of-the-art methods, such as failure mode and effects analysis (FMEA)[28] or fault tree analysis[29]. The downside of these methods, while they are sound and provide a basic overview about the most critical risks present in a system, is that they are lacking in realism, as they use a rating that is based only on severity, occurrence and detection ratings. Our approach will in addition use mathematical techniques to model more important criteria of such systems, notably availability, dependability, reliability and performance. Possible techniques that are of concern here are, for example, reliability block diagrams, Markov chains, fault trees, reward models and Petri nets[30]. This enables the modelling of risk development in the extended perimeter of the utility provider that

[27] Schaeffer-Filho, P. Smith, A. Mauthe, D. Hutchison, Y. Yu and M. Fry, "A Framework for the Design and Evaluation of Network Resilience Management," in 13th IEEE/IFIP Network Operations and Management Symposium (NOMS 2012), Maui, Hawaii, USA. April 2012, pp.401-408
[28] Fadlovich, Erik (December 31, 2007). "Performing Failure Mode and Effect Analysis". Embedded Technology
.
[29] Martensen, Anna L.; Butler, Ricky W.. "The Fault-Tree Compiler". Langely Research Center. NTRS. Retrieved June 17, 2011.
[30] Begain, Khalid; Bolch, Gunter; Herold, Helmut, "Practical Performance Modeling – Application of the MOSEL language", Kluwer Academic Publishers,2001

results in probabilities for certain events and can signal a potentially risky situation to an operator before a severe threat situation develops.

Additionally, the currently used surveillance technologies will be analysed in respect of their adaptability in the case of failures. Here, self-diagnostics will be used to detect system failures and to react accordingly. If the failure leaves the system in a status that still leaves part of the device in an operational state, it may be possible to switch from a normal operational state into a fail-functional state, meaning the system can still perform with a certain impairment, for example by utilising other sensors to extrapolate the necessary data or by interpolating the required data from other surveillance systems remotely covering the area that needs to be protected. While this approach is a possible solution for legacy video surveillance devices, an additional, novel solution will be developed that triggers surveillance on an on-demand basis. The indication to initiate these on-demand devices, such as smartphones of employees (which today are equipped with many different embedded sensor systems), sensor nodes or video monitoring systems, will be given by evaluating the current self-diagnostic data in combination with signalling in the SCADA networks. The former, of course, is with consideration of the privacy rights of device owners. The fusion of these readings allows prediction of the current status of the perimeter infrastructure. The individual wireless connection abilities of these on-demand devices would achieve certain coverage of the perimeter even without a pre-configured networking infrastructure that needs to be set up. By doing so, it is possible either to activate devices to cover certain areas of the perimeter only if the situation requires it, or to enhance an already covered area with additional sensor information to enable a more fine-granular analysis of the situation. However, this of course leads to several issues regarding the communication security and even more the privacy of the devices' owners, which have to be addressed during the project. In a final step, the results gained will be used in dissemination and exploitation activities to develop practical guidelines that can be used by utility providers to enhance their surveillance systems. This can be done by implementing a more sophisticated system to rate and identify threats identified by the existing surveillance systems using the developed models, and/or by enhancing and adopting the proposed novel, on-demand surveillance systems.

[Objective 6] Demonstration and Evaluation of Project Results in Simulated and Real Testbed Environments.

A fundamental objective of HyRiM is the demonstration and the evaluation of Hybrid Risk Management in a real testbed environment. The motivation for this is to ensure that the research output of this project can be adopted by end-users, i.e. utility providers, but also by other stakeholders including legislation, regulation or standardisation bodies. This will be ensured by involving the requests and the demands for our approach from a stakeholder base which will be growing over the course of the project. Additionally, more than a third of the consortium members represent end-user (utility provider) views. These are Akhela from Italy (AKH), a security operator for oil refineries, Linz AG from Austria (LINZ), a multi-utility provider offering a wide range of infrastructures including gas, electricity, heating, water, wastewater and public transport, and the Electrical Cooperative of Alginet from Spain (ECA), an electricity utility. They will direct and guide the implementation of (their) infrastructures in our model to evaluate our project’s approach. They will also shape the outputs we can expect to emerge from our investigations regarding the human factor in cyber risk scenarios. Besides this, real testbeds will be used to study some examples of possible attacks using the ethical hacking procedure applied to a part of these utility networks under realistic conditions. The attacks will first explore the vulnerabilities of the SCADA systems, second will be carried out using personal devices (considering not only of smartphones, but other devices that are typically found in the Internet of Things), and third will explore a combined physical and cyber-attack.
The results of these demonstrations will be evaluated by two different categories of end-users: the utility providers and the consumers. Hence, we will evaluate not only the technical aspects of the metrics and approaches that we develop, but we also consider the influence of the human factor in the acceptance of the proposed methodologies.

The adequate communication and presentation of the results to legislation, regulation and standardisation bodies is also a major goal of the dissemination activities in the HyRiM project. Therefore, a number of workshops will be held to provide state-of-the-art concepts and knowledge to these institutions. The aim is to support European standardisation bodies in providing general guidelines for utility providers to advise them on how to enhance the security of their infrastructure. Additionally, we want to raise awareness at the utility provider's side with the help of these regulation and standardisation bodies.

[Objective 7] Increase awareness of policy makers and pave the way for new legislation and pre-standardisation efforts.

In order to ensure that our research addresses topics that benefit society, we involve utility providers, as well as reaching out to regulatory and standardisation bodies, in our project. New approaches for protecting utilities may require new legislation and standardisation guidelines. Hence it is of fundamental importance to the applicability of our approaches to discuss with the legislation and standardisation bodies how we would introduce the outcomes of our research to them.
Our scientific output will therefore be directly useable and easy to implement. This applies especially to the guidelines we will produce to describe how new approaches to risk assessment or surveillance enhancements can be applied. We plan to organize workshops for which we invite policy-makers and people and organisations involved with legislation and standardisation development, such as ENISA. Reporting on real test cases and on the involvement of end-users of our approaches will shape how new policies, legislation and standards will be created.

1.1.3. Relevance to Topics Addressed by the Call

Table 1 below lists the topics mentioned in the call and explains how they will be addressed by HyRiM.

Topics in the call	Topics addressed	Objective Number
The research output is therefore expected to provide a clear categorisation of critical infrastructures in terms of threat sensibilities versus the impact on the population.	A core activity in HyRiM will be the development of Hybrid Risk Metrics (and Management approaches); these metrics will exhibit properties which will allow their users to apply methodological categorisations, and related methodologies.	1
The task is to develop processes and policies to prevent new threats trends (like for instance Advanced Persistent Threats - APT) targeted against Supervisory Control and Data Acquisition (SCADA) systems. A special attention should be given to the use of new ways of voluntary or involuntary transmissions through personally owned digital / communication devices used in business day to day life.	We will apply our analytical results, as a basis of our investigation, to specific attack scenarios in order to develop tools to help end-users, i.e. specifically for utility providers to manage cyber risks arising from multiple different critical situations.	2
The research should also propose to include these particular threats in existing risk assessment methodologies	HyRiM will also cover the identification and detailed analysis of the SCADA-related attack characteristics and Hybrid Risk Metrics in SCADA attack scenarios, based on existing research projects and	3

	scientific publications. Based on this identification and characterization, HyRiM will define in detail the application of Hybrid Risk Metrics in defence measures, These implies the application of centralized, decentralized or combined security-enforcing policies and protection systems; and countermeasure processes. On the other hand, HyRiM will also design and develop different tools for Hybrid Risk Management in SCADA networks. Based on the investigation and extensive analysis of the previous tasks about the SCADA attacks, different algorithms, mathematical models, programming libraries, and software for assessing cyber risks in SCADA networks will be designed.	
The task is to develop processes and policies to prevent new threats trends (like for instance Advanced Persistent Threats - APT) targeted against Supervisory Control and Data Acquisition (SCADA) systems. A special attention should be given to the use of new ways of voluntary or involuntary transmissions through personally owned digital / communication devices used in business day to day life.	As in technical approaches to cyber risks (e.g. Mobile Device Management in BYOD scenarios) we will investigate the impact on cyber risks deriving from the human factor. We will produce guidelines on how to improve organisational structures and regulation for which we will also consider our Hybrid Risk Management approach.	4
Moreover global guidelines on enhancing the surveillance of these critical infrastructures should be assessed and also new innovative methodologies and technologies should be developed in order to minimise the cyber risks and threats to these systems.	HyRiM will investigate and classify current and novel on-demand surveillance solutions which will – in combination with hybrid risk metrics – enable a utility provider to enhance the ability to predict and react to developing risk situations in its extended perimeter more effectively by employing novel, on-demand surveillance technologies.	5
It is expected that the operators will gain a better understanding of risks against their own infrastructures and minimise cyber risks and threats through new and innovative technologies.	In order to ensure that our approach is easily applicable to existing infrastructures, we will involve stakeholders such as utility providers from the start. They will feed in their requirements and contribute test scenarios to achieve a maximum benefit of our work for society.	6
It is also expected to increase the awareness of policy makers and to pave the way for new legislation if needed. It should also prepare standardisation activity in this area with a view to facilitate an EU market.	New approaches may require new legislation, regulations or standardisation as existing ones may not cater for approaches that we develop. Hence we plan to involve regulator, legislative and (pre) standardisation bodies in the project, through direct engagement and via dissemination events and workshops.	7

Table 1: Relation of call topics to HyRiM objectives

1.2. Progress Beyond the State of the Art

1.2.1. Quantitative Risk Assessment

Conventional risk assessment is often done in qualitative rather than quantitative terms for reasons of efficiency, and often because of practical obstacles, when the necessary figures for a quantitative analysis are hard to get accurately. Commonly, risk is estimated using the standard rule:

Risk = (potential damage of an incident) x (likelihood of this incident),

which reasonably defines risk as "expected damage", but has severe practical issues. For example[31], if the likelihood of a lightning strike is estimated at around 1.24×10^{-6}, and the potential damage is valued at no more than 10,000 €, then the risk (i.e. the expected loss) according to the above formula would work out at 0.124 €, giving the obviously dangerous perception that there is no need for any protection against lightning strikes. The problem here is caused by the likelihood of the incident depending on the context of the system, especially its dynamics and interconnectivity. For a consistent approach, one would in addition need to account for uncertainties in the likelihood and damage, thus creating a two-stage (Bayesian) generalization of the above rule of thumb.
In this regard, coupled complex networks have been studied over the past years; however, their potential for risk assessment is far from fully understood or exploited up till now. Coupled complex networks analysis provides a mathematical framework to study percolation dynamics in systems of two or mode interdependent networks that are subject to cascading failure[32].
Confirmed by extensive numerical simulation of the stochastic process under examination, recent studies show that certain types of interdependent networks are significantly more vulnerable than their non-interacting counterparts in both cases of random failures[33] and targeted attacks[34]. Although results from complex networks research have been applied to some limited cases of real-world networks (e.g. world-wide seaport and airport networks[35]), a mathematical framework to study a specific real-world scenario has not yet been considered. Utility networks are often coupled with other utility, control and financial networks, resulting in a system of interdependent networks.
By applying complex networks techniques to study the vulnerability of utility networks, one can provide a quantitative analysis that assesses the consequences and risks of targeted attacks and random failures in these networks. Finally, this framework can also provide a quantitative approach for designing robust utility networks, also in combination with game-theoretic modelling.
The difficulty to obtain precise and reliable figures for a quantitative risk assessment is the main reason why the German Federal Office of Information Security (BSI) recommends qualitative risk assessment (e.g. based on risk scoring matrices, etc.) instead of quantitative risk assessment, although the need for the latter has clearly been recognized[36]. However, complex coupled network analysis can exactly help in this regard, thus unlocking the full potential of quantitative risk assessment. More importantly, it can objectivize quantitative inputs that are to be estimated subjectively in other competing risk management systems[37].
Qualitative risk assessment does have the appeal of efficiency and is easy to communicate and explain to stakeholders; however, there are no commonly accepted ratings for safety and security

[31] Isabel Münch: *Wege zur Risikobewertung*, in Schartner, P. & Taeger, J. (Eds.): DACH Security 2012, syssec, pp. 326-337 (2012)
[32] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, Nat. Phys. 8, 40 (2012)
[33] S. V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, and S. Havlin: *Catastrophic cascade of failures in interdependent networks*. Nature 464, 1025 1028 (2010)
[34] X. Huang, J. Gao, S.V. Buldyrev, S. Havlin and H.E. Stanley: *Robustness of interdependent networks under targeted attack*. Phys. Rev. E (R) 83, 065101 (2011).
[35] R. Parshani, C. Rozenblat, D. Letri, C. Ducruet and S. Havlin: *Inter-similarity between coupled networks*. Europhys. Lett. 92, 68002 68006 (2010).
[36] R. R. Henning*: Security service level agreements: quantifiable security for the enterprise?*, in proceedings of the 1999 workshop on new security paradigms, ACM, pp. 54-60 (1999)
[37] C. J. Alberts und A. Dorofee: *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley Longman Publishing Co. Inc. (2002).

that would apply as a standard. Existing standards[38] are valuable collections but mostly survey best practices that generally lack a sound theoretical foundation. Further complications arise from the need to map an existing utility network infrastructure to a fixed terminology with which the chosen risk assessment method works. Ontologies[39,40] for that matter have been designed, and tools like AURUM[41] or others based on the Bayesian paradigm[42] or Dempster-Shafer evidence theory[43] have been implemented. Common to all these proposals is their reliance on accurate adversary models and a potentially vast amount of training data. Game-theory on the contrary elegantly avoids these needs by presuming the attacker's behaviour to be optimal in the minimax sense. That is, no matter how the adversary actually behaves, game-theory will always look for the worst-case scenario, so that a sharp assurance for the risk can be established[44].

Most importantly, hybrid risk measures are understood as a multi-criteria risk assessment technique, similar to existing frameworks[45], which attempt to cover safety and security in a single risk assessment process. The HyRiM project is as well related to CORAS[46], which allows integrating multiple risk assessment techniques in the process, yet our envisioned method explicitly accounts for the interplay between different goals due to the use of game-theory.

Complex network modelling and stochastic techniques help to model the known system dynamics and to capture its inherent uncertainty. However, if no such interplay is explicitly known, then game-theory fills the remaining modelling gap by having its conclusions rest only on known outcomes in multiple dimensions of the underlying system, with the hidden dependency structure being implicitly accounted for by the (dependent) safety and security indicators that we consider for risk estimation. In other words, where the interplay is known, we can use an explicit model behind our risk assessment, whereas at stages or parts in the system with unknown internal dependencies or mutual influences, the system performance indicators capture the interplay sufficiently accurately for risk assessment. This combined (hybrid) approach is new and as yet unknown in the literature.

Closely related to our intended hybrid risk metrics, at least on a theoretical level, is the notion of Pareto-optimal security strategies[47,48]. Informally, this is the best defence against an adversary whose possible actions are known, but whose particular behaviour remains hidden to the defender. This notion has been generalized[49] towards a broader class than matrix games, which renders the notion suitable for the more complicated dynamics found in utility networks.

---

[38] Risikoanalyse auf der Basis von IT-Grundschutz (German BSI Standard 100-3), ISO/IEC 27005:2011, „Information security risk management" ISO/IEC JTC1/SC27, ISO/IEC 31000:2009 „Risk Management – Principles and Guidelines on implementation", ISO/IEC 31010:2009 „Risk management – Risk assessment techniques"

[39] S. Kollarits, N. Wergles und H. Siegel et al., *MONITOR – An ontological basis for risk management*, (2008). [Online]. Available: http://www.monitor-cadses.org.

[40] T. J. Chiang, J. S. Kouh und R. I. Chang: *Ontology-based Risk Control for the Incident Management*, International Journal of Computer Science and Network Security, vol. 9, No. 11, pp. 181, (2009).

[41] A. Ekelhart, S. Fenz und T. Neubauer: *Automated Risk and Utility Management*, in Proceedings of the Sixth International Conference on Information Technology: New Generations, IEEE Computer Society, pp. 393-398 (2009).

[42] F. Foroughi: *Information Security Risk Assessment by Using Bayesian Learning Technique*, in Proceedings of the World Congress on Engineering, Bd. 1, International Association of Engineers, pp. 2-6 (2008).

[43] N. Feng und M. Li: *An Information Systems Security Risk Assessment Model under Uncertain Environment*, Applied Soft Computing, vol. 11, No. 7, pp. 4332-4340, (2010).

[44] T. Alpcan and T. Başar: *Network Security: A Decision and Game Theoretic Approach*, Cambridge University Press, (2010).

[45] T. Aven: *A unified framework for risk and vulnerability analysis covering both safety and security*, Reliability Engineering & System Safety, Bd. 92, Nr. 6, pp. 745-754, (2007).

[46] EU Project Nr. IST-2000-25031, CORAS - Risk Assessment of Security Critical Systems, [Online]. Available: http://www2.nr.no/coras/, (2003).

[47] M. Voorneveld: *Pareto-Optimal Security Strategies as Minimax Strategies of a Standard Matrix Game*, Journal of Optimization Theory and Applications, vol. 102, No. 1, pp. 203-210, (1999).

[48] D. Ghose und U. R. Prasad, *Solution concepts in two-person multicriteria games*, Journal of Optimization Theory and Applications, vol. 63, No. 2, pp. 167-189, (1989)

[49] S. Rass: *On Game-Theoretic Network Security Provisioning,* Springer Journal of Network and Systems Management, (2012)

Distinct ontologies for risk assessment [39,40,50,51] may create difficulties when risk diversification or general security precautions in a utility network are to be gauged. Game-theory gives an inherent degree of freedom in defining the performance indicator, i.e., the security and safety measure can be defined in units that the end-user may choose according to his own particular needs. This means that not only existing vulnerability scoring and risk assessment ontologies can be used with the proposed method, but also new taxonomies or standards can be plugged into the methodology. So as an envisioned outcome of the project, different risk assessment taxonomies can be tested for their usefulness and practicality by stakeholders (a question that seemingly has been left entirely unconsidered in the literature except for the ISO and BSI documents listing known best practices), and can subsequently be standardized in a follow-up initiative to the project.

Gaps and limitations in the state-of-the-art	How HyRiM innovates
Risk is often considered as a one-dimensional value, assessed using a set of best-practice techniques.	We will work towards the establishment of a multi-criteria risk view.
Quantitative risk assessment often relies on figures that are hard to elicit accurately	We will derive inputs for a quantitative risk analysis from uncertainty models based on known system dynamics that can be modelled with only little uncertainty.
Risk assessment often prescribes a pre-defined yet hardly standardized vocabulary or taxonomy, into which the system under investigation must fit. Standardized taxonomies may collide with the prescribed vocabulary, thus potentially ruling out standard conformance a priori.	The decision-theoretic approach (game-models) allows for a customizable taxonomy, so as to assure that the risk is measured in units that the end-user (stakeholder) can define to optimally suit the given utility network. Hence, it is easy and efficient to communicate risk valuations. Moreover, suitable taxonomies can be standardized and subsequently used with the method.

1.2.2. Risk Assessment Tools and Methodologies

Traditional probabilistic risk assessment (cf. also the introductory paragraph of the previous section on quantitative risk assessment) has been criticised for an inherent lack of account regarding the complex interplay (indirect non-linear feedback relationships) between system components; this is a property that characterises severe security and safety incidents. It has been claimed [52] that it is "conceptually impossible to be complete in a mathematical sense in the construction of event-trees and fault-trees. This inherent limitation means that any calculation using this methodology is always subject to revision and to doubt as to its completeness"; an argument that cannot fully be refuted, even in the light of advanced research results in this area[53]. Hybrid Risk Metrics will be designed to exactly overcome the gaps of missing interdependency dynamics modelling by relying on explicit models for the interplay where possible (based on probability theory) and using game-theoretic behaviour optimization against unpredictable adversaries elsewhere and in connection with the former. In any case, probabilistic risk assessment rests on the absence of unexpected failure modes. While a residual risk of such event cannot be ruled out in general, proposals to forecast vulnerabilities and risk are surprisingly rare. Reference class forecasting[54,55]is a technique that

[50] Forum of Incident Response and Security Teams (FIRST): *Common Vulnerability Scoring System (CVSS-SIG),* http://www.first.org/cvss/cvss-guide.html (2012)
[51] F. Innerhofer-Oberperfler and R. Breu: *An empirically derived loss taxonomy based on publicly known security incidents*, in: Proceedings of the International Conference on Availability, Reliability and Security, IEEE Computer Society Press, pp. 66-73 (2009)
[52] M. V. Ramana: *Beyond our imagination: Fukushima and the problem of assessing risk*, Bulletin of the Atomic Scientists, (19 April 2011).
[53] P.A.S. Ralstona, J.H. Grahamb, J.L. Hieb: *ISA Transactions 46* ISA Transactions vol. 46, pp. 583-594 (2007).
[54] D. Kahneman and A. Tversky: *Prospect theory: An analysis of decisions under risk*, Econometrica, 47, pp. 313–327 (1979)
[55] D. Kahneman and A. Tversky: *Intuitive Prediction: Biases and Corrective Procedures*, In S. Makridakis and S. C. Wheelwright (Eds.), Studies in the Management Sciences: Forecasting, 12, Amsterdam: North Holland, (1979).

predicts future trends based on past observations. It thus falls under the larger framework of probabilistic forecasting, which we are going to utilize in the project towards building a comprehensive view on potential future threats to which current systems can be adapted in a timely way. As risk management is being embodied in any reasonable business process, especially in the context of utility provisioning, various theoretical approaches and support (partially automated via software) is available[56,57,58,59], among which is one provided by the Austrian Institute of Technology. All these tools follow the ISO guidelines, recommendations and best practices[60]. Nevertheless, most standards and recommendations favour qualitative risk management, thus implicitly discouraging more fine-grained metrics, and the process of risk forecasting and vulnerability modelling is only supported by comprehensive lists of past experience and vague recommendations. Reference architectures and theoretical proposals for securing SCADA systems are available[61,62,63], which emphasize the benefit of automated tool support in the way envisioned in the project[62]. It appears nevertheless unsatisfactory that the literature seemingly contains only reference workflows and general recommendations about how a risk management process should look [64]. The interplay between components and vulnerability/risk propagation is included only implicitly via threat and countermeasure identification.

For decision making, especially in cases where expensive security precautions are planned, quantitative risk assessment is difficult to implement in a process whose performance indicator is the value of risk (VoR) or return of investment (ROI). Existing recommendations and reference architectures appear to intentionally circumvent such quantitative analysis in favour of an easier-to-apply qualitative risk assessment and generic architecture. While arguments in favour of qualitative risk assessment (cf. previous sections) are strong, it remains questionable if decisions can reasonably be based on vague qualitative terms. A point where this appears, nevertheless, to be unavoidable is the human factor's role within a utility network, something that we explicitly pay attention to in a separate work package. The project is in line with ongoing research and community efforts[65], and we further attempt to improve over these in the sense of going more into the architectural details and their implied dynamics found in SCADA networks. The focus in HyRiM will be a theoretically well-founded support for several steps throughout the overall risk management process, whose general structure (if not all the details) agrees with the vast majority of literature in this field. So, instead of proposing yet another risk management process, the project will help refine the details of established and practically proven risk management processes, so as to push the applicability and security of SCADA networks beyond the current state-of-the-art.

[56] Idaho National Laboratory: *SAPHIRE – Systems Analysis Programs for Hands-on Integrated Reliability Evaluations*, https://saphire.inl.gov/ (2012)

[57] ControlScada.com: *SCADA Cyber Security Risk Assessments Tools*, http://www.controlscada.com/ (2012)

[58] IBM: *SCADA Security Solutions*, http://www-935.ibm.com/services/us/en/it-services/scada-security-solutions.html (2012)

[59] Federal Office for Information Security (BSI): *Grundschutztool (GSTOOL)*, https://www.bsi.bund.de/ContentBSI/gstool/gstool.html (2012). The BSI website also provides a list of related and competing tools under https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/AndereTools/anderetools_node.html (2012)

[60] ISO 31000, ISO 31010, ISO 27005

[61] Juniper Networks Inc.: *Architecture For Secure SCADA and distributed control system networks*, http://www.juniper.net/us/en/local/pdf/whitepapers/2000276-en.pdf (2012)

[62] M. Hentea: *Improving Security for SCADA Control Systems*, Interdisciplinary Journal of Information, Knowledge, and Management, vol. 3 (2008).

[63] Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience, IT Security Expert Advisory Group (ITSEAG): *Generic SCADA Risk Management Framework for Australian Critical Infrastructure,* http://www.tisn.gov.au/Pages/default.aspx (March 2012).

[64] Office of Electricity Delivery & Energy Reliability: *21 Steps to Improve Cyber Security of SCADA Network*, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[65] American Business Conferences, Managing SCADA Security Risks (Summit), http://www.managing-scada-security-risks.com (2011)

Gaps and limitations in the state-of-the-art	How HyRiM innovates
Tool support for risk management is usually quantiative and in terms of a fixed risk or vulnerability teminology/taxonomy.	Our tools will be designed to work with a customisable taxonomy for risk management, so as to be compatible with the widest possible variety of standards or even company-specific business processes.
Risk management processes do not or only implicitly define the need and processes to identify risks arising from interdependencies of components, although this has been recognized as a major reason for the severity of recent safety and security incidents.	We aim to provide explicit processes as well as theoretical and practical tools and guidance on how to understand and model the dynamics inherent in a utility network, so that implications of security or safety incidents can be assessed more easily.
Risk management processes are for the sake of generality, kept at a low level of detail, specifying only the coarse steps but offering little guidance on how to accomplish a particular step along way.	Several work packages are dedicated to the instantiation of the theoretical results obtained in WP1; thus providing example applications on one hand, but also direct tool support to put the method into practice in a given setting.

1.2.3. Consideration of the Human Factor

The most relevant recent scholarship on organisational vulnerability and resilience is the work on the 'high reliability organisation' that originated in contexts such as nuclear power generation[66][67] but has been extended into such settings as railroad operations[68] and healthcare[69] - and critical infrastructures in general[70]. But this work concentrates on systems in which there is a single dominant technology - neglecting settings in which, for example, quite different kinds of infrastructure such as power distribution and telecommunications operate in tandem.

The most relevant research on the emergent phenomena that occur in social groups that are threatened with some crisis (such as the loss of a critical infrastructure) is probably that on the social amplification of risk[71] and related ideas including availability cascades[72]. But such ideas are highly general, presenting attempts to understand social responses to a wide range of risk issues. They provide little insight into the unique problems of those involving utilities and the particular threats that loss of service, or some other crisis such as contamination, pose to public risk perception.

There is a wide-ranging understanding of how vulnerabilities develop over time, through long-term processes as well as static structural weaknesses. For example, we know that many technological vulnerabilities are created by legacy systems and 'reverse salients' in technology[73], and equally that many social vulnerabilities are created by patches and revisions in rules, procedures and social agreements[74]. Similarly, we know about problems of 'risk migration'[75], where countermeasures often introduce their own sources of vulnerabilities. But again this knowledge is of a generalized

[66] T.R. La Porte and C.W. Thomas: *Regulatory compliance and the ethos of quality enhancement: surprises in nuclear power plant operations*. Journal of Public Administration Research and Theory, vol. 5, pp. 109-137 (1995).

[67] M. Bourrier: *Organizing maintenance work as two American nuclear power plants*. Journal of Contingencies and Crisis Management, vol. 4, pp. 104-112 (1996).

[68] E.M. Roth, J. Multer and T. Raslear: *Shared situation awareness as a contributor to high reliability performance in railroad operations*. Organisation Studies, vol. 27, pp. 967-987 (2006).

[69] R. Blatt, M.K. Christianson, K.M. Sutcliffe and M.M. Rosenthal: *A sensemaking lens on reliability*. Journal of Organisational Behavior, vol. 27, pp. 897-917 (2006).

[70] P. Schulman, E. Roe, M. van Eeten and M. de Bruijne: *High reliability and the management of critical infrastructures*. Journal of Contingencies and Crisis Management, vol. 12, pp. 14-28 (2004).

[71] R.E. Kasperson, O. Renn, P. Slovic, J. Brown, J. Emel, R. Goble, J.X. Kasperson and S. Ratick: *The social amplification of risk: A conceptual framework*. Risk analysis vol. 8: pp. 177-87 (1988)

[72] T. Kuran and C.R. Sunstein: *Availability cascades and risk regulation*. Stanford Law Review 51, pp. 683-768 (1999).

[73] T. Hellstrom: *Critical infrastructure and systemic vulnerability: towards a planning framework*. *Safety Science*, vol. 45, pp. 415-430 (2007)

[74] J. Rasmussen: *The role of error in organizing behaviour*. Ergonomics, vol. 33, pp. 1185-1200 (1990).

[75] R.E. Alcock and J.S. Busby: *Risk migration and scientific advance: the case of flame retardant compounds*. Risk Analysis, 26(2), pp. 369-382 (2006)

kind, and makes little reference to the unique aspects of utilities and their provision of critical infrastructures. A particular aim in the project is to explore a more hybridised concept of organisational effects. In particular: 1) we will be investigating how organisational phenomena create vulnerabilities in some respects but resilience in other respects - often the two appear to occur together and it is important to study them together; 2) we will be investigating organisational phenomena in the content of combined technological networks (for example, a transportation network in combination with a telecommunications network).
A further goal is specifically to understand social response to utility crises through surveys and modelling. This should provide insight into how the particular aspects of such crises can stimulate public reactions, and how such reactions either exacerbate or moderate such crises.
Known solutions to problematic scenarios in which actions towards risk mitigation unwittingly introduce new vulnerabilities, will be applied specifically to utility networks. Utility networks offer particular challenges in terms of incorporating legacy systems and integrating diverse technologies, and it is important to find ways of modelling such characteristics in developmental models.

Gaps and limitations in the state-of-the-art	How HyRiM innovates
Much research focuses on a single dominant technology, leaving aside settings that incorporate different kinds of infrastructure (and their interplay).	We will conduct explicit studies of organisational phenomena that create additional vulnerability via an attempt to create more resilience elsewhere. This work will be done with a focus on combined technological networks and incidents that occur together (thus exhibiting non-negligible interdependencies).
Relevant research on emergent phenomena related to crisis management in social contexts is highly general and provides little insight to the specifics of utility networks.	We will conduct interviews and empirical research to gain insight into the dynamics of crisis evolution and its public perception, especially regarding utility networks.
Studies on vulnerability evolvement and propagation are general and contain a considerable number of general sources of risk, while making little attempts to apply these ideas to practical settings in utility networks.	We will bring theoretical ideas into practice by applying known theory to utility networks. Challenges in utility networks are different and new, so that current theoretical frameworks need adaption and extensions, to which HyRiM will contribute.

1.2.4. Surveillance Technologies for the Extended Perimeter in Utility Infrastructures

Surveillance technology is one of the key approaches to obtain real-time data. This data can be used to measure and quantify the parameters needed for a precise risk calculation. The results are then used to derive suitable countermeasures to reduce the risk. However, smaller utility providers in particular make only very limited, or no use at all, of surveillance technology to protect their networks and extended perimeter infrastructure at the same time. In particular, most actions are limited to the reaction to already occurred incidents, e.g. power or gas outages. Hence, the current state-of-the-art can be summarized as reactive. To overcome this limitation, the HyRiM project will investigate novel surveillance technologies along with a categorization and classification approach. These also cover the questions where and how these systems can be used in the area of utility networks and facilities. This will help to detect and avert potential risks before they lead to an incident that can impact both the utility provider's infrastructure as well as being potentially harmful to employees or customers, i.e., the functional safety aspects are considered as well. The utility provider then has the chance to proactively reduce risks instead of just reacting to incidents, which increases the reliability and sustainability of existing and future utility networks. Moreover, state-of-the-art assessment of risks is mainly done by static methods, such as failure mode and effects analysis (FMEA)[76], or fault tree analysis[77]. While these methods are sound and provide a basic overview about the most critical risks present in a system, they are lacking in realism, as they rely on an abstract rating[78]. To tackle this lack of realism, the current risk assessment methodologies will be improved by not only using the standard techniques, but by developing new approaches.

[76] Fadlovich, Erik (December 31, 2007). "Performing Failure Mode and Effect Analysis". Embedded Technology.
[77] Martensen, Anna L.; Butler, Ricky W.. "The Fault-Tree Compiler". Langely Research Center. NTRS. Retrieved June 17, 2011.
[78] Kmenta, Steven; Ishii, Koshuke (2004). "Scenario-Based Failure Modes and Effects Analysis Using Expected Cost". Journal of Mechanical Design 126 (6): 1027. doi:10.1115/1.1799614.

These will be able to improve current models by rating other important system criteria, notably availability, dependability, reliability and performance utilising appropriate modelling methodologies. Possible techniques that are of interest are, e.g., reliability block diagrams, Markov chains, fault trees, reward models and (stochastic) Petri nets[79]. One of the major improvements using such modelling approaches is that not only an abstract rating of a risk is visible, but a concrete probability of a live system can be seen. In addition, the development of a risk over time can be monitored and evaluated, which in turn allows the possibility of reacting to a potentially dangerous situation before a serious threat can develop. Surveillance of perimeters comes in many flavours, e.g. the current trend in video surveillance technologies is moving from conventional CCTV video surveillance to interconnected camera systems using IP networking technologies. While these systems are easily manageable and provide features such as standard monitoring, recording, event detection and forensic analysis (license plate and face recognition), they still have to be carefully set up and configured, and they tend to remain static and inflexible in their operation. In addition, such surveillance systems are responsible for ensuring the continuous operation of other systems, making their reliability of the utmost importance. However, if surveillance is used inside the extended perimeter of a utility provider, it is additionally located in a potentially hazardous, unsupervised environment. This increases the risk of an undetected failure, which can be caused by various events, such as temporary or permanent hardware failures, software errors, accidents, vandalism or planned attacks. Currently, the possibilities to detect a system failure are mostly limited to visual inspection after the damaged system is identified and replaced. In addition, an appropriate reaction to such a system impairment that ensures that the overall protection is not severely impacted is still not readily available. HyRiM will investigate the causes and implications for surveillance system failures by using methodologies such as fault tree analysis and FMEA (failure modes and effects analysis). Deriving from the results of such techniques, it will be possible to prepare effective detection- and counter-mechanisms.
In HyRiM, both the lack of flexibility and the potential failure of current surveillance systems will be addressed by the introduction of novel, on-demand surveillance technologies, which can be used to increase perimeter and network security. These novel technologies (such as wireless sensor networks, cell phones or other networked device using appropriate sensors) will have the advantage that they are highly mobile and flexible. This flexibility opens up the possibility of using dynamically active specific sensors inside of a wireless sensor node, depending on the current situation inside of the perimeter. This would have the benefit that devices are only used on an on-demand basis, reducing cost and overhead compared to an “always-on” solution. We will also investigate what the impacts of the new surveillance network on the existing infrastructure are. In particular, it is not clear how the utility networks are interacting with the surveillance infrastructure, e.g. what happens in case of outages. To trigger such on-demand surveillance systems, the currently available surveillance data will be used in combination with other data sources, such as SCADA networks, to be able to activate additional devices to either enhance the current surveillance in a certain area or to replace impaired surveillance systems.

Gaps and limitations in the state-of-the-art	How HyRiM innovates
Surveillance technologies are currently only sparsely used to monitor the whole perimeter of a utility provider.	HyRiM will investigate novel surveillance technologies along with a categorisation and classification of arising risks.
Current state-of-the-art risk modelling methods lack realism, as they only provide an abstract rating.	In the HyRiM project, the current risk assessment methodologies will be improved to produce more meaningful results.
State-of-the-Art surveillance technology is focusing on IP-Networking, which causes new dependencies on the underlying networks.	The approaches developed in HyRiM will derive new methods to integrate and sustain novel surveillance technologies within the utility networks.
Currently, the reaction to incidents in the surveillance area is limited to visual inspection of the damaged system.	HyRiM will investigate mechanisms for determining the causes of failures.

[79] Begain, Khalid; Bolch, Gunter; Herold, Helmut, "Practical Performance Modeling – Application of the MOSEL language", Kluwer Academic Publishers,2001

1.2.5. Related Projects

Table 2 lists relevant related projects and their relationship to HyRiM.

Project	Summary	Link to HyRiM
PRECYSE	Methodology, architecture, technologies and tools to improve the security, reliability and resilience of the design of ICT systems supporting critical infrastructures. *EU-FP7-project coordinated by ETRA with AIT is a partner.*	PRECYSE targets industrial control systems. ETRA and AIT are members for both projects. This ensures that a part of the results will be exchanged between the projects partners. Furthermore, this will also increase the impact of research results to the users of critical infrastructure.
SERIMA	Design of tools aiding the quantitative assessment of security in a given information infrastructure. Therefore, algorithms coming from game theory are applied which provide a risk measures that can be set up in any unit or context suitable for the application at hand. *National Research Project coordinated by AIT.*	SERIMA provides an elementary mathematical framework for risk metrics based on a game theoretic approach. Although risk assessment is based on communication networks only, a similar mathematical concept can be used as a basis for the development of Hybrid Risk Metrics in HyRiM.
RSB	Development of a method based on game theory for risk analysis in communication networks within or among critical infrastructures for several security goals that explicitly takes interdependencies between these goals into account. *National Research Project coordinated by AIT.*	RSB is the thematic follow-up project to SERIMA and hence provides deeper insights into risk assessment based on game theory. As in SERIMA, the security is classified in terms of a multivalued (vector-valued) yet only static risk metric that leaves system dynamics aside. HyRiM will improve and innovate by taking the system dynamics into account, plus not being primarily about designing novel communication protocols.
$(SG)^2$	Systematic study of smart grid technologies in terms of ICT security issues and the research of countermeasures. Based on a thorough threat and risk analysis from a state-level perspective and security analysis of Smart Grid components, $(SG)^2$ explores measures for power grid operators that serve to increase the security of computer systems deployed in the future critical infrastructure of "energy". *National Research Project coordinated by AIT.*	$(SG)^2$ focusses on Smart Grids, which represent only one part of the utilities targeted in HyRiM. Interconnection to other utilities is not a topic in $(SG)^2$. Both LINZ AG and AIT are involved in this project which guarantees that synergies between the two projects can be used. Such synergies might be, for example, the identification of threats and vulnerabilities in connection with Smart Grids. However, in contrary to $(SG)^2$ HyRiM follows a well-founded mathematical approach (i.e. game theory and Bayesian theory) regarding risk assessment and risk metrics.
MASSIF	MASSIF (Management of security information and events in service infrastructures) monitors and correlates security-related events in an attempt to predict future intrusions at an early stage. It does so by monitoring, e.g. process activities, to detect misbehaviour and raise alerts. The output comprises security architectures, security notifications and actions as well as countermeasures.	HyRiM, unlike MASSIF, will primarily be focused on utility networks, and approaches similar goals with entirely different tools. In particular HyRiM's focus on interconnected networks goes beyond the topics discussed in MASSIF. The output of HyRiM concerns similar items as MASSIF, but HyRiM is not primarily on incident notifications but on security metrics. Some of MASSIF's

		work items are covered by the surveillance work packages in HyRiM, but again, using different techniques than MASSIF.
CORAS	Development of a base framework applicable to secure critical systems that supplies customisable, component-based road maps to aid the early discovery of security vulnerabilities, inconsistencies and redundancies. Further, CORAS provides methods to achieve the assurance of the security policy implementation.	Like CORAS, HyRiM will develop a toolset for risk analysis and risk management. CORAS, however, does not cater for interdependencies between security goals in interconnected networks, which is a core focus of HyRiM.
OCTAVE	OCTAVE (Operationally Critical Threat, Asset, and Vulnerability of Evaluation) uses employee's knowledge to assess and define the current state of the security, and uses fault/event tree analysis to achieve a defined improvement.	The Human Factor is one major security aspect in HyRiM. Hence, interviews and fault/event trees are two among other methods that HyRiM will base its security metrics on.
MICIE	Establishes a warning system for critical infrastructures to identify, in real time, the level of possible threats.	Threat prediction is a duty in HyRiM and warnings can be issued based on the derived security metric. HyRiM is, however, not about rapid alerting a priori.

Table 2: Related projects and their links to HyRiM

1.3. S/T Methodology and Associated Work Plan

To achieve the objectives mentioned in the above section, the HyRiM Project includes a) Research and Development (RTD) activities to carry out investigations of theoretical fundamentals, scenario-specific applications, and considerations of the human factor and perimeter protection. It also includes b) Demonstration (DEM) activities during which our research outputs will be applied in realistic scenarios with the involvement of stakeholders. To coordinate the research efforts as well as the demonstration activities HyRiM of course also includes c) Management (MGT) activities which cover the administrative management and the technical management during the implementation of the project, to ensure that the research goals of the project are met within the administrative boundaries of time and budget. Finally, d) Other (OTHER) activities include the dissemination and exploitation of RTD and DEM achievements and results, and the planning and setting up of measures to maximize the societal and industrial acceptance of the HyRiM solutions.

HyRiM is structured into seven work packages (WPs), in which the main activities are carried out, with four WPs are RTD, one WP is DEM, one WP is MGT, and one WP is OTHER.

1.3.1. The Overall Strategy of the Work Plan and Work package interdependencies

As illustrated in Figure 2, WP 1 will provide the theoretical foundations which will be refined by the partial outputs of WPs 2, 3 and 4 in order to ensure its applicability in real-world scenarios. This will feed into the evaluation, assessment and demonstration of results in WP5. Additionally, there is a feedback process from WPs 2, 3 and 4 to theoretical foundations of WP 1. This ensures that the theoretical framework of WP1 can be adopted if necessary using insights coming from the real-world scenarios of WPs 2, 3 and 4.

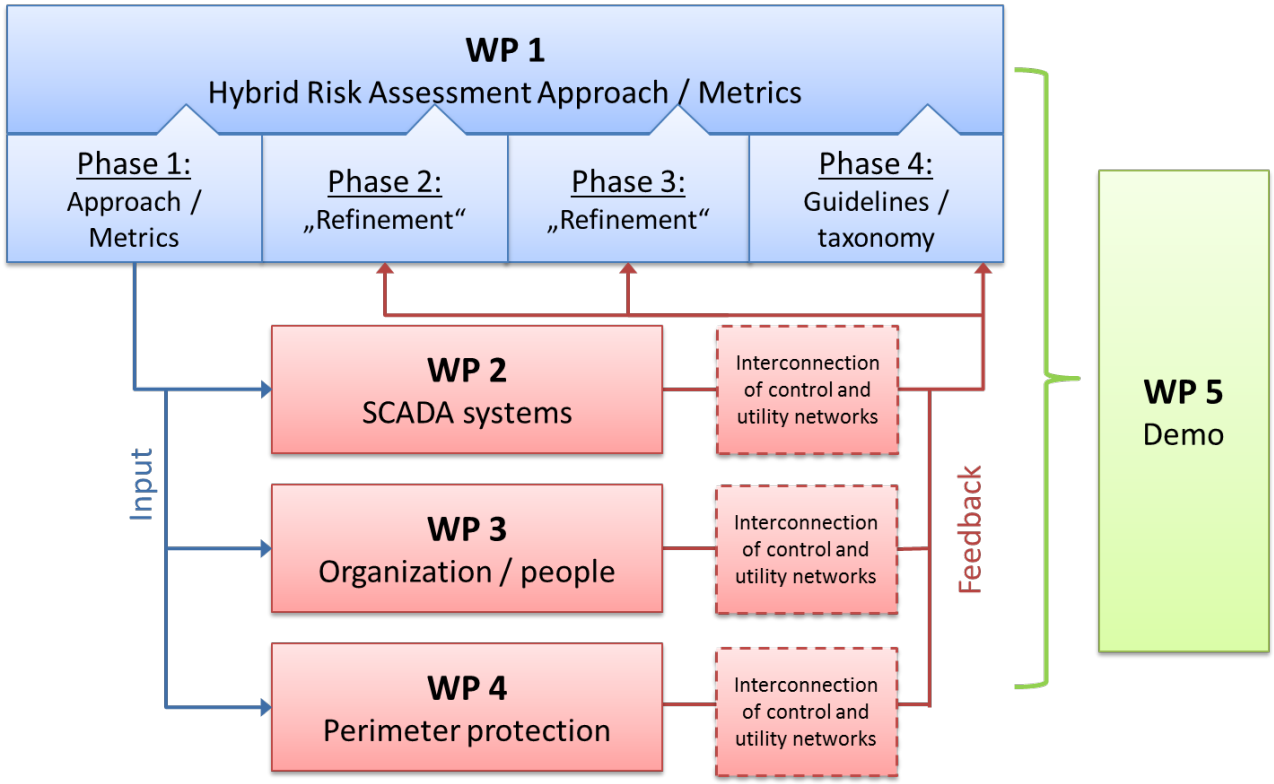

Figure 2: HyRiM Work Package Correlations (w/o Management and Dissemination WP)

1.3.2. Detailed work description

Work package list

Can be found in Part A – WT1

Summary of staff effort

Can be found in Part A – WT6

Deliverables list

Can be found in Part A – WT2

List of project Milestones and Outcomes

Mile-stone (MS) #	Milestone Outcomes	WP(s) in-volved	Exp. date [80]	Means of verification and related Deliver-able (D) [81]
MS1	(Cyber) Risk trends identified	WP1	M8	(Cyber) Risk trends in D1.1 finished
	Project-website	WP6		Project website in D6.1 finished
	Legal and Ethical Compliance verified	WP7		Report in D7.6 submitted
MS2	Operator requirements and (cyber) risk trends identified	WP1	M12	Report in D1.1 submitted
	SCADA-related attacks characterised	WP2		Report in D2.1 submitted
	Dissemination activities in first project period	WP6		D6.1 submitted
MS3	Mathematical description of Hybrid Risk Metrics provided	WP1	M18	Report in D1.2 submitted
	Relevant organisational factors identified	WP3		Report in D3.1 submitted
	Surveillance-related threats and coun-termeasures listed	WP4		Report in D4.1 submitted
	ELAB status report of first project period	WP7		Report in D7.7 submitted
	Review of management activities in first project period	WP7		First EC Evaluation passed
MS4	Categorisation of vulnerabilities given	WP1	M24	Report in D1.3 submitted
	HRM framework extended to SCADA networks	WP2		Mathematical framework in D2.3 finished
	Influence of surveillance on Hybrid Risk Metrics identified	WP4		Collaboration between HRM and surveil-lance in D4.3 defined
	First exploitation plan	WP6		D6.4 submitted
	Dissemination activities in second project period	WP6		D6.2 submitted
	Software tools for Hybrid Risk Metrics in SCADA networks	WP2		Software in D2.3 provided
MS5	Reference architecture model specified	WP3	M30	Report in D3.2 submitted
	Analytical framework and metrics defined	WP 3		Report in D3.4 submitted
	Enhancement of perimeter surveillance support defined	WP4		Report in D4.3 submitted
	Demo use cases identified	WP5		Use cases in D5.1 described
MS6	Customer and utility provider surveys finished	WP5	M36	Report in D5.2 submitted
	Demo results provided	WP5		Report in D5.3 submitted
	Final exploitation plan	WP6		D6.5 submitted
	Standardisation activities	WP6		D6.6 submitted
	Dissemination activities in third project period	WP6		D6.3 submitted
	ELAB status report of second project period	WP7		D7.8 submitted
	Review of Management activities in sec-ond project period	WP7		Third EC Evaluation passed

Table 3: List of project Milestones and Outcomes

[80] Measured in months from the project start date (month 1).

[81] Show how you will confirm that the milestone has been attained. Refer to indicators if appropriate. For example: a laboratory prototype completed and running flawlessly; software released and validated by se-lected end-users; field survey complete and data quality validated.

1.3.3. Work plan and timetable

To ensure a project life cycle which allows the iterative refinement of the theoretical foundations as shown in Figure 2, we plan the specific WPs to exhibit an overlap. This is simplistically illustrated in Figure 3 (the Gantt chart, below) and individual tasks are explained in more detail thereafter.

A detailed visualisation of the interdependencies between the different tasks (T) of the work packages in the Gantt chart would not be possible without losing its readability. Therefore, the following table shows preconditions necessary for a specific task to start. Preconditions are in all cases related to milestones (MS). They however do not need to represent the final deliverable required for the milestone; they can also represent preliminary results which are then being fed into a task.

Task	relies on	Preconditions	Milestone
T1.4	T1.3	Preliminary mathematical model of Hybrid Risk Metrics defined	MS2
T2.2	T1.3	Preliminary mathematical model of Hybrid Risk Metrics defined	MS2
T2.4	T2.2	Preliminary mathematical model of Hybrid Risk Metrics for SCADA networks defined	MS3
T3.2	T3.1	Organisational factors within utility providers identified	MS3
T3.4	T3.1	Organisational factors within utility providers identified	MS3
T3.5	T3.1	Organisational factors within utility providers identified	MS3
T4.2	T1.1	List of current and future threats compiled	MS1
T4.3	T1.3	Preliminary mathematical model of Hybrid Risk Metrics defined	MS2
T4.3	T4.1,T4.2	Preliminary list of threats detectable by surveillance technologies compiled	MS2
T4.5	T4.4	Preliminary list of applications compiled	MS3
T5.2	T2.3,T2.4	Preliminary tools and applications for Hybrid Risk Metrics on SCADA networks identified	MS4
T5.2	T3.4,T3.5	Preliminary monitoring framework and reference architecture identified	MS4
T5.2	T4.4,T4.5	Preliminary applications of Hybrid Risk Metrics to support surveillance identified	MS4
T5.3	T5.1	Involvement of end-users described	MS6
T5.4	T5.1	Involvement of end-users described	MS6
T5.5	T5.3,T5.4	Preliminary results from surveys described	MS5

The activities in tasks T1.3, T2.3 and T4.4 partly rely on results coming from their direct predecessors, i.e. T1.1, T2.2 and T4.3. Looking at task T1.3, the mathematical definition of the Hybrid Risk Metrics needs at some point input from task T1.1 but not at the beginning. Hence, results coming from T1.1 can be incorporated into T1.3 later on.
Regarding tasks T2.3 and T4.4, the implementation performed in these tasks builds upon the results of the theoretical framework they are based on. Conversely, the validation of the theoretical framework relies on prototype implementations. Hence, these tasks are running with a large overlap to be able to use the results of each other interchangeably.

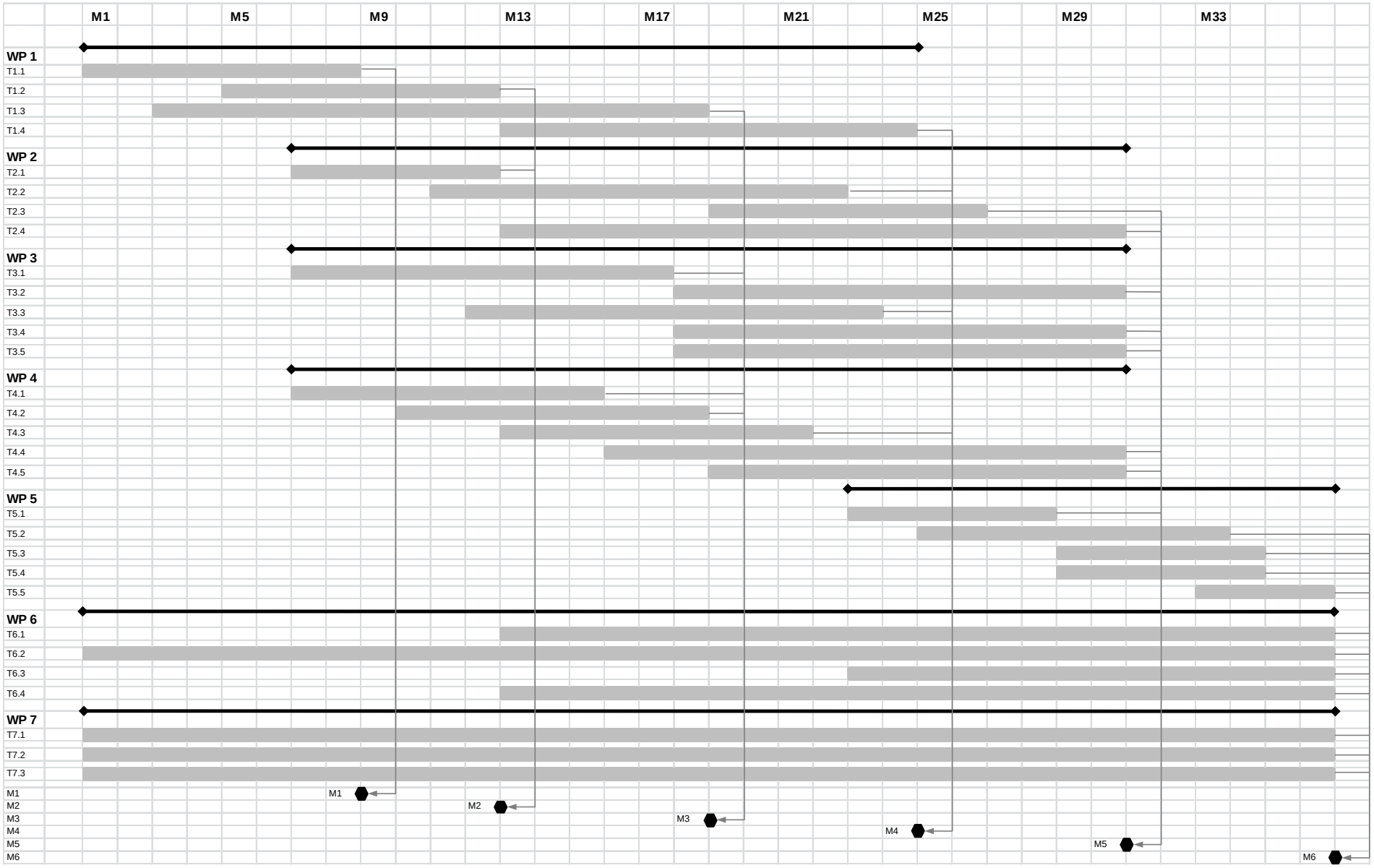

Figure 3: HyRiM GANTT chart

The Gantt chart is simplified in order to enhance readability. Not all and results flowing into a milestone are shown. For a detailed description of the milestones, please refer to the milestone list above.

			Lead	Contr.	AIT	ULANC	UNI PASSAU	ETRA	AKH	ECA	LINZ	Total
WP1	**Hybrid Risk Metrics and Methodology for Risk Assessment**				**25**	**12**	**17**	**20**	**9**	**10**	**6**	**99**
	T 1.1	Trend analysis of (cyber) risk on utility networks	ULANC		1	6	9	4	3	7	4	**34**
	T 1.2	Deriving requirements from utility providers	ETRA			3		8	4		2	**17**
	T 1.3	Definition of hybrid risk metrics and assessment methods	AIT		24		5	4				**33**
	T 1.4	Categorisation of vulnerabilities based on Hybrid Risk Metrics	ETRA			3	3	4	2	3		**15**
WP 2	**Hybrid Risk Assessment for Interconnected Utility Networks**				**20**	**15**	**7**	**25**	**9**	**0**	**2**	**78**
	T 2.1	Identification of SCADA-related attack characteristics as wells as mitigation and p	ETRA		6	6	7	14	2		2	**37**
	T 2.2	Definition of a Hybrid Risk Metric in SCADA attack scenarios	AIT		8	3		5	2			**18**
	T 2.3	Provision of tools for Hybrid Risk Management in SCADA networks based on existi	AKH		6	3		3	5			**17**
	T 2.4	Application of Hybrid Risk Metrics in defence measures such as preventative poli	ULANC			3		3				**6**
WP 3	**Human and Oragnisational Risk Analysis**				**5**	**21**	**6**	**10**	**0**	**0**	**2**	**44**
	T 3.1	Investigation of organizational factors within utility organizations	ULANC		1	5					2	**8**
	T 3.2	Investigation of incidents using secondary data	ULANC			5	2					**7**
	T 3.3	Investigation of risk responses in society	ULANC			5	2					**7**
	T 3.4	Development of analytical framework and metrics	ULANC			6	2	4				**12**
	T 3.5	Development of monitoring approaches and a reference framework	ETRA		4			6				**10**
WP 4	**Perimeter Protection Enhancements**				**6**	**5**	**35**	**0**	**18**	**0**	**2**	**66**
	T 4.1	Surveillance Technologies Trend Analysis	ULANC			5	8		3		2	**18**
	T 4.2	Dealing with threats by surveillance	AKH				4		3			**7**
	T 4.3	Application of surveillance to compute Hybrid Risk Metrics	UPASS				5		3			**8**
	T 4.4	Application of Hybrid Risk Metrics and Assessment to support surveillance	UPASS		3		4		4			**11**
	T 4.5	On-Demand Surveillance Enhancement	UPASS		3		14		5			**22**
WP 5	**Evaluation and Assessment of Project Results in Simulated and Real Testbed Environments**				**2**	**5**	**7**	**17**	**21**	**14**	**6**	**72**
	T 5.1	Identification and involvement of end-users	AKH		2	5		4	12	7	6	**36**
	T 5.2	Definition of use cases	AKH					4	6			**10**
	T 5.3	Surveys with regards to user acceptance	ECA					3		4		**7**
	T 5.4	Survey with utility providers	ECA					2	3	3		**8**
	T 5.5	Evaluation, preparation and presentation of results for policy and decision make	UPASS				7	4				**11**
WP 6	**Dissemination, Exploitation and Impact**				**14**	**5**	**3**	**14**	**7**	**3**	**4**	**50**
	T 6.1	Workshop with utility providers and policy makers	AIT		6			3	1	1	2	**13**
	T 6.2	Dissemination Activities	UPASS		4	4	2	3	1	1	1	**16**
	T 6.3	Liaison, standardisation and regulation activities	ETRA		2			4	2			**8**
	T 6.4	Exploitation Plan	AKH		2	1	1	4	3	1	1	**13**
WP 7	**Project Management**				**23**	**0**	**5**	**0**	**3**	**0**	**0**	**31**
	T 7.1	Legal and Financial Management	AIT		13							**13**
	T 7.2	Management of Project Execution	AIT		10				3			**13**
	T7.3	Management of Legal, Ethical, Privacy and Policy Issues	AIT				5					**5**
Total PM					**95,0**	**63,0**	**80,0**	**86,0**	**67,0**	**27,0**	**22,0**	**440,0**

Table 4: Breakdown of HyRiM staff effort

2. Implementation

2.1. Management structure and procedures

The HyRiM project management provides a focused, lean but effective framework to support the partners in achieving the scientific and technical objectives of the project. Efficient decision-making processes and swift responsiveness to changing circumstances are required. This is what the theory says, but it is not so easy to achieve since experience shows that outstanding – and very often too complex – quality management plans fail simply because they are very difficult to apply in practice.

In the following section, it is described how HyRiM will put all these principles and the specific strengths and constraints of HyRiM consortium into operation from a very pragmatic perspective.

The goal has been to define a management structure and a set of principles and procedures which, whilst being as flexible, agile and cost-efficient as possible, leave as little room as possible for subjective interpretation.

2.1.1. Management Structure

The work to be done within HyRiM is structured into a set of work packages. Each work package is divided into tasks, and each task is led by a Task Leader (TL).
The Project Coordinator (PC) takes responsibility for the overall project management. This includes interactions with the European Commission on contract-related issues as well as chairing regular management meetings. The PC has amongst his responsibilities a set of administrative and financial tasks - representing the project in the contract negotiation, and in relation to the Commission's Project Officer, representing the consortium in workshops and official meetings, collecting administrative reports from partners and forwarding periodical reports to the Project Officer, preparing and updating the consortium agreement between the participants, administering project resources and project spending, managing the overall ethical and gender issues, co-ordinating the exploitation of the project's results, etc. The PC shares his technical responsibilities – monitoring the overall performance of the project, managing the technical audits, supervising the preparation of the final deliverables – with the Technological Manager (TM).

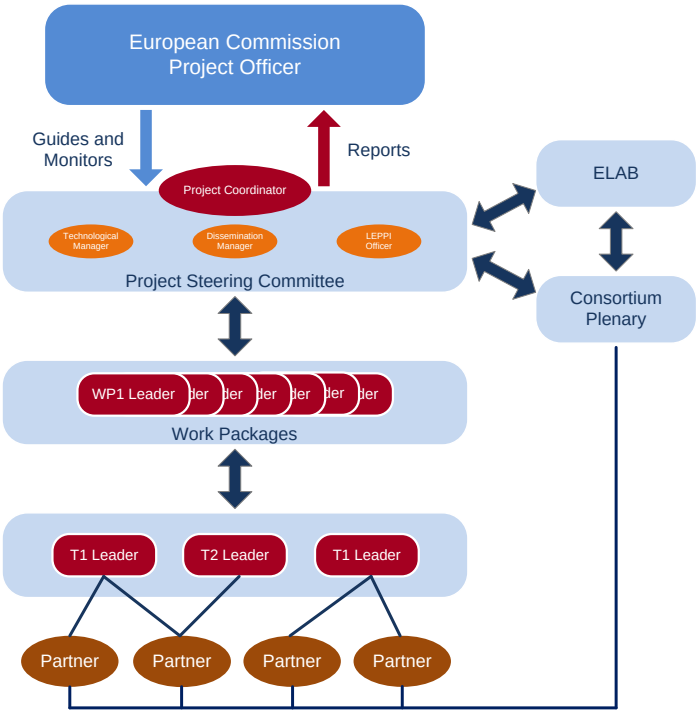

Figure 4: HyRiM project management structure

The TM is one of the main members of the Project Steering Committee (PSC). The PSC has responsibility together with the Coordinator, for monitoring the overall progress and direction of the project, the resources used, the costs incurred and risk evaluation. Reasons for any deviations from the project plan will be identified and the necessary corrective actions will be agreed by the PSC. Any differences between participants will be resolved by the PSC as they arise. Major changes in the project plan, such as reallocation of resources, may be done within the limits of agreements, by the decision of the PSC as put forward by the Project Coordinator.

The PSC will convene at least every three months, in order to provide quick and efficient response to the events that will arise during the project. The PSC meetings will precede the Plenary Meetings in order to prepare for them. Whenever possible, the PSC will use remote meeting technology.

Jointly with the PC and the TM the Dissemination Manager (DM) and the LEPPI complete the PSC. Other persons may attend to the PSC meetings as advisors by invitation –either consortium members or external experts – with voice but without voting rights. The PSC meeting's date and agenda will be announced by the Project Coordinator at least three weeks prior the meeting.

The Dissemination Manager (DM) will be the coordinator of all the project dissemination activities. He/she will be supported in all the relevant decisions by the Project Coordinator, and they will collaborate in the definition of the project website structure and functionalities, being part of the project website a Project Library, i.e. a collaboration working space for the exchange, sharing and storage of project documentation (deliverable, white papers, agendas, minutes, reports, etc.). ´

Regarding Legal, Ethical, Privacy and Policy Issues (LEPPI) a designated LEPPI Officer together with the independent Ethical and Legal Advisory Board (ELAB) will be the institution addressing possibly arising problems related to legal, ethical, privacy and policy issues. In particular, the LEPPI Officer will be in charge of coordinating and supervising the execution of all LEPPI related decisions and recommendations of the ELAB (cf. Section 2.1.5 and Annex A below for details).
Regarding issues of quality management a separate Quality Manager (QM) will be selected from the staff of the partner responsible for quality management, i.e. Akhela (AKH). The Quality Manager will support the Project Coordinator and the Steering Committee in ensuring the achievement of the entire quality of the Project (cf. Secition 2.1.2 below for details).

The PSC will be supported in the different work packages by work package leaders (WL). A WL will be responsible for all the actions in the WP, following the description of activities and objectives specified in the project plan, as well as for carrying out the respective deliverables on time, and ensuring no delays in the accomplishment of the tasks. WLs will co-ordinate the activities within the work packages and will work in close co-operation with the Project Co-ordinator.
Within each work package the Task Leaders (TL) will be the responsible person for the day-to-day work needed to carry out the tasks related to their specific activity. Their coordination work is not subject to any additional administrative or reporting burden; instead they will act as team leaders of all the individuals from the different partners involved in a specific task.

Last but not least, all the partners will be represented in the Consortium Plenary (CP). The CP is the key liaison between the project and partner organisations. In the CP meetings the Project Co-ordinator will present the project's status and plans for the next period. Representatives of the partner organisations will be able to voice their opinions and ask for more detailed information on progress and plans. The CP meetings will take place twice a year and, if possible, in conjunction with the scientific and technical dissemination activities of the project. Dates of the meetings will be announced by the Project Coordinator at least eight weeks prior the meeting.

Function	**Company**	**Person Name**
Project Coordinator, WP7 Leader	AIT	Christian Monyk
Technological Manager	AIT	Stefan Schauer
LEPPI Officer	UNI PASSAU	Hermann de Meer
Quality Manager	AKH	Carla Cannas
WP1 Leader	AIT	Stefan Schauer
WP2 Leader	ETRA	Lola Alacreu Garcia
WP3 Leader	ULANC	David Hutchison
WP4 Leader	UNI PASSAU	Hermann de Meer
WP5 Leader	AKH	Katiuscia Zedda
WP6 Leader, Dissemination Manager	ETRA	Lola Alacreu Garcia

2.1.2. Quality management

The quality management of the project will be overseen by a certified Quality Manager selected from the staff of Akhela, who will ensure the quality of the management and other internal processes in the project. The Quality Manager has the overall quality responsibility for the project and provides support to the Project Coordinator regarding the quality management. He/she is responsible for the quality of the documents delivered from a development perspective.
The main responsibilities of the Quality Manager are:

- Design and implementation of the Quality Assurance Plan that will contain rules and procedures that the project will have to follow in order to guarantee the highest possible quality
- Revision and pre-approval of the deliverables
- Support the Project coordinator in ensuring the achievement of the required quality of the project
- Identifying and proposing suitable correction in case of non-conformity.

The quality assurance plan will be described in a separate deliverable (D7.2) due at the beginning of the project (month M3).

The quality of the project management is ensured by preparing a project handbook, the first version of which will be prepared by the Project Coordinator and accepted by PSC by M3. The project handbook will be based on this section of the document.
The project handbook will describe the roles of different actors in project management, meeting schedules and template agendas for Plenary and PSC meetings and will give guidelines for performing the day-to-day project management actions, including:

- instructions and templates for technical reporting;
- instructions and templates for administrative reports;
- templates and naming/numbering conventions for technical and administrative files and documents.

As a part of this project handbook, the project will apply an internal reviewing procedure to guarantee the quality of its results. Each WP leader will be responsible for the quality of the results – especially deliverables - of his WP, which will be subject to a peer review by at least two experts, one of whom will be another WP leader – the one who will take as input the results of the WP being reviewed.

WP #	**Leader**	**Reviewed by…**	**WP #**	**Leader**	**Reviewed by…**
WP1	AIT	UNI PASSAU, ETRA	WP5	AKH	AIT,ECA
WP2	ETRA	AKH, AIT	WP6	ETRA	ECA, AKH
WP3	ULANC	UNI PASSAU, AIT	WP7	AIT	ULANC, UNI PASSAU
WP4	UNI PASSAU	AKH, ULANC			

The project handbook summarises all the contact points for each partner, email lists, web sites and other essential information. The latest version of the project handbook will be available on the HyRiM web site. It is expected that this document will be updated annually based on the experience gained.
Since the HyRiM objectives are ambitious, an exact planning cannot be elaborated in advance to cover the project's life span. This makes continuous planning and refinement of the project plan necessary. It is expected that a full cycle: *planning -> execution -> analysis -> revision -> planning,* etc. should take three months.

<table>
<tr><td></td><td>Partner</td><td>Task leader</td><td>WP leader</td><td>Co-ordinator</td></tr>
<tr><td rowspan="4">Technical</td><td>info =></td><td rowspan="2">Monthly technical reporting =></td><td rowspan="4">Consolidates quarterly =></td><td rowspan="4">Analyses, collects, takes action, reports to EU</td></tr>
<tr><td>info =></td></tr>
<tr><td>info =></td><td rowspan="2">Monthly technical reporting =></td></tr>
<tr><td>info =></td></tr>
<tr><td></td><td colspan="3">Partner</td><td>Co-ordinator</td></tr>
<tr><td rowspan="3">Administrative</td><td colspan="3">costs, person months, eventual changes; monthly =></td><td rowspan="3">Analyses, collects, takes action, reports to EU</td></tr>
<tr><td colspan="3">costs, person months, eventual changes; monthly =></td></tr>
<tr><td colspan="3">costs, person months, eventual changes; monthly =></td></tr>
</table>

Table 5: Monitoring and reporting practices

The monitoring will be based on specified document forms provided by the coordinator and collected via email or web.

2.1.3. Risk management

A number of risks are relevant to the project, which might cause the delay in achieving milestones, in the worst case, partially jeopardize the project. Also, in a project that involves different organisations, it is likely that problems occur with respect to the collaboration and joint execution of work packages. It is important that potential risks are clearly identified and assessed, and that recoverable actions and procedures are defined that can be instantiated if needed.

Since risks may occur at any time in project development, a constant risk monitoring activity is needed. In HyRiM, whenever a risk or signals of a potential risk is spotted, the first step is to clarify the potential problem. This is in essence a first level risk analysis (mainly qualitative) aimed to make relevant aspects emerge and provide to the relevant involved actors enough info to conduct a specific and careful analysis of risk nature. The same aspects, but in much more detail will be taken into account also in the quantitative analysis bringing to the actual risk classification (quantitative).

Thus the project management of HyRiM provides a number of mechanisms to identify and resolve potential risks. In HyRiM, we identify the following groups of potential risks:

- Partner Problems: e.g. a partner is underperforming or a key partner is leaving the project
- Expertise Risks: e.g. a key person with a specific expertise is leaving the project
- Project Execution Risks: e.g. key milestones or critical deliverables are delayed
- Agreement Risks: e.g. consortium partners cannot agree because of different interests
- Competition Risks: e.g., a competing solution comes up and makes the results less valuable.

Risk management will be used as a means to systematically manage the uncertainty within HyRiM in order to increase the likelihood of meeting the objectives and execute the project based on the baseline plan. The project management team will continuously monitor and control the execution of the project according to the project plan with its milestones and critical paths. In addition, HyRiM will employ a monthly reporting scheme, which ensures that the project management team is aware of potential problems on a monthly basis, and can initiate countermeasures long before a problem becomes severe. The tight control both at work package level and at overall project management level ensures that measures and solutions will be put into place in time.

Major aspects in HyRiM to look at are:
activities affected – which are the activities on which the risk may impact and which are the activities that may have originated the risk;

- actors affected – which may be the affected actors;
- potential impacts – which are the potential impacts on affected activities and actors;
- actors involved – which are the involved actors (those directly involved in the activities that may have ingenerated the risk), which are the actors that have identified the risk and which could be the actors managing it;
- potential reasons/causes – what have been the most probable causes for the issue;
- potential solutions – what are the possible remediation actions (in core).

Based on the project risk management method, in the planning phase, HyRiM has identified the following significant risks and the associated contingency plans.

	Risk Description	Prob.	Impact	Precautions	Contingency Plan
Partner Problems					
PP1	Despite the partners' determination to participate in the HyRiM project, various external events may cause a partner to withdraw their participation.	Low	Medium	Within the consortium and the work packages the partners have complementary tasks and skills. However, there is a degree of overlaps in the partners' expertise in case of a partner withdrawal.	At first the project coordinator will try to shift resources released by a partner to another member of the consortium capable to fulfil the abandoned tasks. Furthermore a list of candidate institutions able to replace a partner will be compiled at the beginning of the project, which will be used in the case of any partner changes. The resources released by a partner will then be used to find a replacement via a short-term contract or subcontracting. This will be discussed in the Steering Committee.
PP2	One or more partners, force a lack of resources and/or personnel changes upon the project.	High	Medium		A positive and constant communication between project coordinator and other partners maximizes the chances to detect these possibilities at an early stage. The issue is then raised with management in partner organisations as soon as possible to guarantee clear situations for all partners.
PP3	Participating end-users face problems in providing a demo platform based on a real life scenario	Low	Medium		The specification and preparation of the demonstrators will be started in an early phase of the project, which gives more time to negotiate and overcome any eventual difficulties. In addition, the Advisory Board provides possibilities for integrating additional demonstration scenarios.
Expertise Risk					
E1	HyRiM might not generate the expected impact in standardisation bodies and relevant interest groups.	Medium	Low	HyRiM is keen in influencing standards and the relevant interest groups as well as industry bodies and therefor plans a tight integration of industry partners and standardisation bodies in the project.	The project will pursue all relevant ways to secure the promotion of the project results at relevant venues. The tight integration of industry partners and Advisory Board in the project will offer the opportunities to demonstrate the project results in realistic settings and enable interactions with the industry to promote and increase project impacts.
E2	HyRiM may not be able to get access to required hardware facilities to integrate or test the HyRiM risk management tools under realistic conditions.	Low	Low	HyRiM aims at developing platform independent solutions and the mapping from generic concepts to specific implementation to overcome the heterogeneity of existing technologies used at the various utility providers.	Timely scheduled organisation of the needed infrastructure gives the possibility to find alternative solutions in time if a problem occurs.

Project execution risk					
PE1	Despite responsible calculation there might be the risk of wrong estimation of required effort for the fulfilment of project tasks.	Low	Low	The HyRiM proposal and its work plan have been carefully partitioned into detailed tasks to enable, as precise as possible, the estimation of required PM.	In the event of redistribution of effort this will be made in accordance with standard procedures defined by the Commission.
PE2	Since HyRiM wants to maximize the possible impact on standards and industry it has to consider failure in capturing all threats, attack characteristics and utility provider's requirements.	Low	Low	The consortium has carved out various key topics and requirements the project should address. These can effectively be used to monitor the progress in capturing all relevant information.	The HyRiM project will involve all stakeholders from the beginning of the project, and implement an iterative process to ensure that all relevant requirements will be captured and further refined during the early stages of the project. The integration of the Advisory Board at various stages of the project also ensures the correct collection and communication of threats, attack characteristics and requirements.
PE3	Deadlines of milestones and deliverables might be missed.	Low	Medium	This risk has been considered in the technical management in WP7. Major project milestones are coupled with deliverables; furthermore, most deliverables are phased with a draft due half way through the project.	The project coordinator monitors the progress on different deliverables, tasks and work packages on various levels continuous through the projects' development.
PE4	Milestones and deliverables might be delayed putting back the schedule.	Low	Medium	Critical project paths have been analysed and can be addressed specifically.	Resources will be regrouped to address critical tasks with particular effort. In the case of missing requirements the team will focus on the key requirements. Progress monitoring throughout the project will be in place to detect possible risks at an early stage.
PE5	The adoption of the project results might not comply with the agenda.	Medium	Low	Various tasks of dissemination are scheduled at an early project phase with different entities.	Dissemination of projects results, extended dissemination activities, standardisation activities, and liaison with standardisation bodies are expected to be handled since an early phase of the project
Agreement Risk					
A1	Possible IPR problems and reluctance to release and share information within the consortium.	Low	Low	The partners are familiar with their commitments within an EU project since most partners have been involved for years in EU research and development.	A Consortium Agreement will be signed, regulating these concerns internally.
Competition risk					
C1	There is a risk that methodologies regarding the underlying risk management for utility providers might progress in a different direction from the envisaged framework.	Low	Low	The partners bring extensive knowledge in the area of risk management for utility providers as well as the underlying methodologies. This makes a solid analysis of the current situation and the most probable developments possible.	However, the technical work within the project will constantly monitor the related developments and adopt any major new development.
C2	Due to the fact that surveillance is a very fast developing field, there exists the possibility, that technological developments in the time between the projects' proposal and the actual start of the project render the project out of scope.	Medium	Low		The task leaders will examine their work items with respect to most recent technology evolvements at the beginning of the project as well as in the time of the project.

Table 6: Risks and contingency plans

During the initial project phase, a more detailed list of risks and associated project impact as well as indicators and potential activities to manage these risks will be prepared. Risks will be classified with respect to their probability of materialising to a real problem (low, medium, high), the possible impact (low, medium, high) and a strategy to eliminate or reduce the risk. In case a risk related to research and technological development cannot be eliminated or reduced a fall-back strategy will be defined. Technical and organisational risks will be covered.

A dedicated person will dynamically monitor and reassess defined and potentially emerging (new) risks and adapt the risk management plan and evaluate the effectiveness of measures taken to reduce risks. An update of the risk assessment and management report will be delivered every 6 months.

2.1.4. Security management

Security management constitutes an important part in this project; hence, the focal points issued in this context are the following:
A group should be set up with representatives from within the Consortium and including the end users with sufficient knowledge of security issues, to monitor regularly the project and to assess the sensitivity of all deliverables, esp. D1.2, D2.1, D2.2, D 3.1, D3.2, D4.1, D4.2, D4.3, D5.2, D5.3, D3.3, D2.3, D 6.1 - 6.3. - It is recommended that this group monitors whether the results of the research are likely to generate classified information and make sure that no classified background information will be used inside the project. A special clause on limited dissemination (to the Consortium and the end users) should be included into the grant agreement.

In the context of the consortium, a S*ecurity Sensitivity Committee (SSC)* will be established to scrutinize the various security-related aspects pertaining to the project's activities. The *SSC* will be made up of the members of the Project Steering Committee (PSC), i.e. Christian Monyk, Stefan Schauer, Hermann de Meer and David Hutchison, as well as end-user members of the HyRiM consortium (ECA, Linz, AKH), i.e. Lola Alacreu Garcia, Carla Cannas and Karl Rossegger, to reflect the importance of the SSC to HyRiM activities, and, in particular, the potential security implications HyRiM activities have in the context of the demonstrator scenarios. The SSC will be led by the project coordinator (AIT). A potential candidate for the chair of the SSC would be Christian Kollmitzer, who is a specialist in applied information security as well as the respective standards used in this project.

The major focus of the SSC is to monitor all security related issues during the project. In particular, this includes assessing the sensitivity of the deliverables and the information therein as well as observing the creation of classified information during research. Additionally, the SSC will make sure that no classified background information will be used inside the project

In detail, the SSC will have the following major duties:

- Report on the sensitivity of the content in deliverables produced by the HyRiM consortium. Prior to the issue of all deliverables, the SSC will assess their sensitivity. The results on this matter will be included in the front matter of all the written deliverables produced by the consortium. A review of the sensitivity assessment will be performed in parallel to the Quality Management process (see Section 2.1.2), i.e., during the same period a deliverable is being subjected to peer review for quality management reasons; it will similarly be re-assessed by the project's SSC to verify the result of the sensitivity assessment.
  Although this process will be applied to all of the HyRiM deliverables, it is understood the following set are of a particularly sensitive nature:

  D1.1 Report on (cyber) risk trends in utility networks and operator requirements
  D1.2 Report on definition and categorisation of Hybrid Risk Metrics
  D2.1 Future trend SCADA-related attack, mitigation and prevention tools
  D2.2 Protection and countermeasure policies and processes
  D2.3 Software tools for Hybrid Risk Management in SCADA networks

D3.1 Analysis of human and organisational factors in utility vulnerability and resilience
D3.2 Development of a reference architecture with associated metrics and monitoring framework
D3.3 Analytical framework and associated metrics
D4.1 Physical and cyber risk prediction modelling using surveillance systems
D4.2 Guidelines on surveillance technologies to secure utility networks
D4.3 How to enhance perimeter security using new surveillance technologies
D5.1 Utility network evaluation guidelines for (cyber) risk investigations
D5.2 Survey regarding consumer and utility provider acceptance
D6.1 Dissemination report year 1
D6.2 Dissemination report year 2
D6.3 Final dissemination report

- The SSC will produce a deliverable in the context of work package 7 on related security sensitivity issues with respect to the project's activities. Specifically, this document will report on the following issues:
  - security sensitivity issues with respect to the trials that are planned as part of WP5 on demonstrations; and
  - specific procedures with respect to the use of cryptographic data in the context of the demonstrator scenarios.

  To give optimum visibility regarding the issues to be addressed in this deliverables, it is proposed to be delivered in M12 of the project.

- On topics regarding the protection of personal data and information, especially gathered during demonstration activities and surveys, the SSC will collaborate closely with the Ethics and Legal Advisory Board (ELAB) and the data controller. This will guarantee compliance with EU legislation and the EU Data Protection Directive (Directive 95/46/EC).

- The SSC will convene at the project's regular Consortium Plenary (CP) meeting, in the context of WP7 on Project Management, to discuss security-related issues that result from the project's current and forthcoming activities. A set of minutes for this will be produced.

- The activities of the SSC will be included in the periodic project reports.

2.1.5. Ethical and Legal management

2.1.5.1 Legal, Ethical, Privacy and Policy Issues (LEPPI) Officer

The LEPPI Officer is Part of the Project Steering Committee (PSC). He is contact Person for addressing possibly arising problems related to legal, ethical, privacy and policy issues. He acts the link between the PSC and the ELAB and also cooperates with the project's appointed data controller to comply with national and EU legislation.

The LEPPI Officer will be in charge of:

- Informing the PSC and the ELAB on reported or recognized LEPPI
- Chairing the ELAB
- Informing the WP leaders on decisions and recommendations of the ELAB with respect to LEPPI
- Coordinating and supervising the execution of all LEPPI related decisions and recommendations of the ELAB
- monitoring of decisions made by the ELAB with respect to LEPPI
- Dissemination (as part of the activities in WP 6) of HyRiM best practices with respect to LEPPI applied during the project

2.1.5.2 Data Controller

The project's appointed data controller (according to Directive 95/46/EC and 1/2010 Opinion of the Article 29 Working Group) with respect to the HyRiM project will be ULANC. The data controller will "determine(s) the purposes and means of the processing of personal data" (according to Art. 2 (d) Directive 95/46/EC) and cooperate with the LEPPI Officer and the ELAB to comply with national and EU legislation. Details on "purposes and means of the processing of personal data" can be found in Section A2 of the Annex.

Each site will also appoint individual a site-specific personal data protection official (according to Directive 95/46/EC) and a site-specific ethics advisor responsible for day-to-day issues and for implementing the decisions of the ELAB. The appointed site-specific personal data protection officials and ethics advisors will be given in D7.6. In the case of subcontracting, the responsible site – and thereby data controller – will provide the instructions given to the data processor in D7.6.

2.1.5.3 Ethical and Legal Advisory Board (ELAB)

Within the framework of HyRiM an independent Ethical and Legal Advisory Board (ELAB) for ethical and regulatory issues will be set up. It will consider the multidisciplinary nature of possibly arising ethical issues. The ELAB will facilitate compliance with ethical requirements by providing guidance on ethics and regulatory issues. Moreover, the ELAB will be responsible for keeping the project partners well-informed about any new ethical regulations relevant to the HyRiM project. Actions will be taken in order to increase researchers' awareness of ethical issues.

Members

HyRiM is a multidisciplinary and interdisciplinary project. Therefore, the ELAB is populated with three experts who can provide information and guidance on cross-disciplinary ethical and data protection issues. Possible candidates would be, e.g., Ruth Fee from the University of Ulster, Peter Tolmie from Nottingham University, Prof. Rob Procter from Warwick University or Hans Zeger from ARGE DATEN. Further, it will consist of employees' representatives, who are selected from members of the consortium. The ELAB is part of the management structure of HyRiM (as depicted in Figure 4) with the LEPPI Officer as its chairman (cf. Section A2 of the Annex).The ELAB will form a direct link with individual regulatory bodies, e.g. the British Sociological Association, the British Psychological Association, German Ethics Council would be considerable, the Bavarian Commissioner for Data Protection and Freedom of Information or the Austrian ARGE DATEN.

Tasks

The ELAB is appointed to oversee the legal and ethical concerns of the project. This includes visiting the research sites, overseeing the development and use of ethical consent forms and forwarding these in deliverables to the Commission as well as ensuring that those partners, who handle sensitive data, are aware of their obligations with regard to confidentiality (ISO/IEC 27001:2005).

The ELAB decides on guidelines and best practices that should be promoted, executed, and monitored by the LEPPI officer with respect to:

- The 'unforeseen usage' implications of the project;
- Ensuring the compliance with the revised Directive 95/46/EC on data protection and privacy;
- Monitoring that the security solutions developed within HyRiM respect European legislation;
- Ensuring that the data protection directives are respected when implementing interconnections of communication infrastructure systems (with respect to the exchange for personal data);
- Promoting awareness on ethical principles and legal requirements within the project work packages;
- Review and approve all human research ethics and legal issues in HyRiM; and
- Review and resolve relevant complaints about HyRiM research issues relating to any adverse events.

The ELAB reports on compliance with the revised Directive 95/46/EC on Data Protection and Pri-

vacy by providing the following reports to the Commission:

- D7.6 within 6 months of commencement reporting on initial compliance with EU directives on informed consent, data and privacy protection ;
- D7.7 within 18 months of the start of the project reporting on the continued monitoring of ethical and legal issues; and
- D7.8 at 36 months reporting on how the project has met required ethical and legal standards.

Detailed information on privacy issues, Data protection and compliance with the EU Data Protection Directive covered by the ELAB can be found in Annex A.

Meetings
The ELAB attends annual consortium meetings, where a special session supervised by the ELAB will be dedicated to ethical and regulatory issues. The ELAB monitors the work performed and advises the HyRiM Project Steering Committee, when necessary. A report from the ELAB will be included as early, intermediate and final project deliverables (cf. Table 3).

Financials
As financial compensation, each of the three members of the ELAB will receive a fee of € 5.303,-- for the complete project runtime, which will be paid in three annual rates. Each of these rates will be paid to the ELAB members one month after their work at the annual project meeting at the latest. The fees will serve as budget for the ELAB members to pay for travelling costs as well as compensation for their work in the ethic and legal decision making processes of HyRiM. Each of the ELAB members will receive a fee contract granting him/her the aforementioned fee, which is financed through the subcontracting budget of UNI PASSAU.
The beneficiaries' representatives will attend the ELAB meetings, as they are co-located with the annual project meetings. Because of that, they will be inherently present at such meetings and will not receive any additional reimbursement.

2.1.6. Knowledge and IPR management

For the operation of a successful project, it is important to have an IPR strategy in place so that all partners of the consortium work collaboratively in a coherent manner towards the achievement of common objectives. The IPR strategy should be focused and very clear in order to best protect the innovations developed within the time-frame of the project from attacks by competitors. This will also help in maximising the returns on the human, capital and intellectual investments.

In addition to the approval procedures for documents, publications and standards contributions the management of knowledge is handled in the **grant agreement**, **rule for participation** and **consortium agreement** between the HyRiM partners.

The management of knowledge and intellectual property and other aspects of innovation in this project are allocated to specific activities within work packages. They are twofold: On the one hand IPR applications for new systems and solutions will be prepared by participants. On the other hand **information will be disseminated within the project and to external bodies** such as publications, presentations and regulatory and standards bodies, ***but only after the necessary steps for ensuring the protection of IPRs have been made. This ensures that intellectual property will be secured in the interest of project partners***. Contributions to external bodies will have an impact on global harmonisation of concepts and systems. The dissemination of information and the influence, e.g. on standards bodies, are the prerequisites for the economic success of IPRs.

The management of such activities will be part of the mandates of the PM and the General Assembly. If required, the General Assembly will adjudicate on difficulties that are drawn to its attention related to knowledge management and associated matters.

2.1.7. Internal and external communications

The international and geographically distributed nature of HyRiM partners emphasizes the importance of using ICT tools for location independent co-working. The tools to be used include:

- a web page with a public area and a private work space;
- news forum and discussion groups;
- mailing lists for general, PSC, WP, and activity members;
- e-drafting, writing, editing and reviewing of documents, including Deliverables and internal reports, and scientific papers, by using email, web site, and collaboration tools;
- net meeting, audio and video conferencing especially for intermediate PSC, WP, and activity meetings;
- besides, cloud services for cooperative work will also be considered, as some experience with such tools is already existing in the consortium and has also been gathered during the project preparation.

Both internal and, especially, external communications will be regulated by the Consortium Agreement, clearly identifying the mechanism to announce the publication of new material – external communications – and the procedures to exchange information within the consortium.

2.1.8. Consortium Agreement

A consortium agreement (CA) will be concluded between the HyRiM partners according to the European Commission checklist recommendations and following the "Rules for the participation of undertakings, research centres and universities in, and for the dissemination of research results for, the implementation of the European Community Seventh Framework Programme (2007-2013)", Regulation (EC) 2005/0277/COD. It will include:

- the internal organisation and management of the consortium;
- intellectual property arrangements;
- settlement of internal disputes;
- any ethical consideration and gender issues;
- the detailed procedure to manage the external and internal communications.

The settlement of the IPR management policy within the project will follow the “Guide to IPR for FP7 projects” published by the EC (28/06/2007) and will result, as previously explained, in an exploitation agreement to be signed by all relevant partners.

2.1.9. Conflict Resolution

Identification of any conflicts which arise in the project lies in the responsibility of each project participants. Any signs of disagreement between project participants should be notified to the task leader, work package leader, or project manager (as appropriate), who should then instigate the conflict resolution procedure, whereas escalating to higher levels should only be done if necessary.

Conflict resolution is as follows:

1. The task/work package/project manager will separately contact all parties to identify the different viewpoints. Based on a clarification of viewpoints, the manager should try to propose a solution. If one is achieved, it will be recorded in short minutes. If no suitable solution for all parties can be achieved, the problem is escalated.
2. If this approach fails, the matter will be taken up to the next level of escalation. Here, the same procedure as in level 1 applies.
3. In the uppermost level, all work should be in writing. If conflicts relate to matters which would normally be assessed as part of the annual reviews by the Commission, the views of the Commission should be sought.

The rational at the back of the need to identify such aspects is just to have the clearest possible picture of the situation so to facilitate the following steps. By no way this has to be intended as a way to identify the “black goat” to blame.

- Internal: it becomes apparent that a partner will not be able to perform the task assigned to him; project costs in a work package are in danger to exceed the amounts foreseen in the contract; etc.
- External: changes in the technology development that may necessitate a change in the goals of the project or of parts thereof; availability of other/new technologies that may make parts of the project obsolete or can be utilised for the project; etc.

Once a risk is confirmed, the project coordinator will install processes to cope with these risks. The envisaged risks at the stage of the project proposal preparation phase and the solutions are listed above (see Table 7). Every possible risk is categorized as described above. They are furthermore rated by probability of occurrence and possible impact.

2.2. Individual participants

2.2.1. Austrian Institute of Technology

The AIT Austrian Institute of Technology GmbH is an Austrian research institute with a European format and focuses on the key infrastructure issues of the future. The AIT Department of Safety & Security focuses on these two important aspects of ever-increasing relevance for today's citizens, which will also take centre stage in the information society of tomorrow.

- "Safety" is in our case related to technologies and refers to the personal safety of individuals, which is directly or indirectly dependent on the proper functioning or availability of an information processing and/or autonomous system.
- "Security" rather refers to the protection of information and the prevention of any potential violation through unauthorized access to or alteration of personal information. Security may also refer to classical security techniques (surveillance) that are supported by IT.

The Department of Safety & Security is making a significant contribution to ICT and is devoting concerted efforts to guaranteeing operational efficiency and reliability of all critical infrastructures – both private and public – especially in times of potential ecological, economic and political crisis. We are committed to fostering the roll-out of national infrastructure as well as the deployment of state-of-the-art technologies in the area of public administration (eGovernment, eEnvironment), power grids, health care (eHealth), transportation networks, payment systems, telecommunications, Internet as well as the business and industrial sector with a view to positioning Austria at the forefront of the European ICT industry.

Competencies: As the largest non-university research facility in Austria, AIT has a long history and outstanding track record on participating and leading EU and national research projects. An important part of the research of the IT Security within the Safety & Security Department is concentrated on secure system design for safety and security-critical information systems. Our current research work includes security aspects in Cloud Computing, security technologies for Service Oriented Architecture with a focus on the efficient implementation of security requirements through model-driven approaches, the development of federated identity management, cyber defences of critical infrastructure, security for smart grid and smart meters, and organisational information security management. AIT is an active member of the European research community, and has participated and also coordinated numerous European research projects. Recent activities of the Safety & Security Department include participation in the FP7 PRECYSE, FP7 SUDPLAN and FP7 ASSETS projects and the coordination of the FP7 SECCRIT and FP7 TaToo projects, among many others.

Main tasks: As the project coordinator, AIT will be in charge of the administrative and technical management of the project. AIT will also participate in the RTD work packages and lead tasks on the definition of Hybrid Risk Metrics and standardisation and regulation activities. In addition, AIT will support the implementation of use cases in the demonstration and contribute to the dissemination, exploitation and impact of the project results, as well as the coordination with the (extended) Advisory Board.

Short profile of key people:

Dr. Stefan Schauer is an experienced "Risk Management"-researcher in AIT's Safety & Security Department. He studied Computer Science at the University of Klagenfurt and received his PhD in Theoretical Physics, working on Quantum Cryptography, at the Technical University Vienna. Since 2005 he is working for the AIT in several projects related to the fields of classical security and risk management. Currently, his main focus lies in the field of risk management and risk assessment as well as security architectures for critical infrastructures. In this context he is interested in risk assessment using game theoretic approaches and the identification and handling of threats coming

from the human factor. He has experience leading medium-sized national research projects funded by the FFG as well as other research promotion agencies.

Dr. Markus Tauber is an AIT Project Manager in the ICT security team in future networks and services of AIT's Safety & Security Department. He is an experienced Project Manager who was working for 8 years at B.net (AT) where he was responsible for e.g. setting up a wireless infrastructure to connect rural areas to the Internet throughout the most eastern part of Austria (Burgenland). B.net was originally established as outsourced infrastructure department of a utility provider which is now named "Energie Burgenland". After his time with B.net and until recently he was working for 8 years as researcher at the University of St Andrews (UK) where he gained academic experience covering various topics in the area networks and distributed systems. This includes a post as Research Fellow working on application specific performance and energy efficiency in WLAN with Prof. Saleem Bhatti which as for the India UK Advanced Technology Center. In 2010 he received his PhD at the University of St Andrews for which he was working on "Autonomic Management in Distributed Storage Systems"

Bernhard Strobl is in AIT thematic coordinator of the program "Intelligent Camera Networks". He graduated in 1986 with an M.Sc. in informatics at the Vienna University of Technology, Austria. He is in AIT since 1987, working on specification, implementation and project management of several industrial projects with focus on hardware and software development for video encoding, decoding, transmission and storage. For AIT he developed a patent[82] of a video encoding algorithm. Currently, his main focus of activity is on video content analytics. He is the manager of several research projects: the AIT internal project "Video Archive Search" and the two national funded projects within the Austrian Security Program: SECRET (Search of Critical Events in Video archives) and SECRET - interactive. He is Member of the ONVIF consortium (Open Network Video Interface Forum).

Dr. Stefan Rass studied technical mathematics (with a focus on statistics), and computer science at the Alpen-Adria Universität Klagenfurt and graduated with a double degree in 2005. He gained a PhD degree in mathematics in 2009 for a dissertation about information-theoretic security. His research interests include (among others) general system security, complexity theory, decision theory and risk management. Past and ongoing national risk management projects like SERIMA or RSB are partially based on his research results. He served the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) as an expert witness.

Dr. Lucie Langer is currently working on projects related to the security of critical infrastructures and smart grids. Before joining the AIT she has been working as a Technology Consultant in the private sector for two years, focusing on access rights and infrastructure management in large-scale IT projects. From 2006 to 2010 she was a member of the Cryptography & Computer Algebra Group at Technische Universität (TU) Darmstadt, where she also received her PhD in 2010 and graduated in Mathematics in 2006. As a Research Assistant at TU Darmstadt she participated in several security-related research projects on e-voting, e-government and long-term archiving.

[82] B.Strobl, B.Bischof, S. Veigl, *Verfahren und Einrichtung zur Übertragung von Bildfolgen*, Komprimierungsverfahren: Selektive Blockdifferenz Patent: Österreich, Nr. 500.721

2.2.2. Lancaster University

Lancaster University is one of the top UK research-led Universities with 92% of its research recognized as world leading or internationally significant in the latest UK Research Assessment Exercise (RAE). The School of Computing and Communications (SCC) at Lancaster University is, according to the UK Engineering and Physical Sciences Research Council (EPSRC) latest landscapes document, one of the leading research centres of excellence in ICT in the UK. The School is internationally known for its leading-edge contributions to networked and distributed systems. Significant research is carried out in the area of resilient networking and the area of wireless sensor networks (WSNs). Lancaster's research work has attracted strong support and collaborations from industry such as BT Labs, Microsoft, Orange, Cisco, HP Labs, France Télécom, Lucent, Intel, Agilent Labs, Telekom Austria, and ETRI in S. Korea. Lancaster is also a central participant in many EU funded research projects, and also R&D projects funded by EPSRC.
Currently a number projects in areas related resilience, risk management and security are being carried out, forming a research environment in which the proposed work can be implemented successfully. Relevant on-going projects include the India-UK Advanced Technology Centre in Next Generation Networks and the EU EINS Network of Excellence in Internet Science in which all of the investigators in the current proposal are involved. In the past several years Lancaster has been part of the EU projects ResumeNet and ANA (David Hutchison) which are relevant to the proposed work. Recently, Lancaster has become one of the eight new Centres for Cybersecurity in the UK, and several new PhD students have started and/or are being recruited in this area of research. In addition, Lancaster has several research activities in the areas of ethnography (Mark Rouncefield) and risk management (Jerry Busby), the former within SCC, and the latter within the Management Science Department in the Lancaster Management School.

Competencies: Within the Computing department these include network resilience and security, and ethnography of human computer interaction. Within the Management Science department this includes risk analysis – ranging from expertise in risk perception and risk amplification, through to the control of risk in hazardous organizations, and specific topics such as the incorporation of intentionality into risk assessment procedures.

Main tasks: Lancaster will have an involvement in several work packages and will lead work package 3. Within work package 3 its main tasks will be to participate in the organizational fieldwork and the secondary data analysis, participate in the consumer surveys and subsequent modelling, and to participate in the development of the analytical framework, related metrics, the monitoring framework and reference architecture.

Short profile of key people:

Prof. David Hutchison is Professor of Computing and Director of InfoLab21 at ULANC. Further, David has been Director of Information Systems Policy at ULANC. Over the years David has built a strong, internationally respected research group in networking at Lancaster, which is well known for contributions in a range of areas including Quality of Service (QoS) architecture and mechanisms, multimedia caching and filtering, multicast engineering, active and programmable networking, content distribution networks, mobile IPv6 systems and applications, wireless network systems, and communications infrastructures for GRID based systems. David has also initiated the resilient networking related research activities at Lancaster that have resulted in five resilience related projects and made ULANC a centre for resilient and dependable networking.

Dr. Mark Rouncefield
Mark Rouncefield is a Senior Research Fellow in the Department of Computing, Lancaster University. He was a recent holder of a Microsoft European Research Fellowship for his work on social interaction and mundane technologies. His research interests involve various aspects of the empir-

ical study of work, organisation, human factors and interactive computer systems design. This work is strongly inter-disciplinary in nature and has led to extensive and continuing collaborations with colleagues in Sociology, Computing, Informatics and Management departments both in the UK and abroad. His empirical studies of work and technology have contributed to critical debates concerning the relationship between social and technical aspects of IT systems design and use. Recent work has focused on socio-technical aspects of the design and deployment of technologies in domestic and healthcare settings. He is particularly associated with the development of ethnography as a method for informing design and evaluation. He has been on the editorial advisory board of the CSCW journal, the International Journal of Organisational Transformation and Social Change (OTSC), Sociological Research Online and the Health Informatics Journal.

Dr. Jerry Busby is a senior lecturer in the Department of Management Science. His research interests are in risk analysis, organisational failure and error making. His work has been funded by the UK EPSRC, Leverhulme Trust, the UK Health and Safety Executive, the UK Maritime and Coastguard Agency, the Nuclear Installations Inspectorate and a number of commercial firms. Most recently this work has included studies of the social amplification of risk, risk migration, risk redistribution, sensemaking about risk controls and organisational degradation. He is associate editor of the International Journal of Risk Assessment and Management.

Dr. Andreas Mauthe is a Senior Lecturer at Lancaster University and has been working in the area of distributed and multimedia systems, content management and content networking for almost 20 years. He has been heading research and development activities in academia as well as industry. Andreas current research focus is in the area of novel infrastructures for content distribution, and autonomic network management and resilient networking. He is on the Editorial Board of the ACM Multimedia Systems Journal, has been participating in standardisation activities (e.g., ISO, SMPTE, VQEG), and served as an expert and evaluator for the European Commission. He has been for instance contributing to the definition of the EU's Future Media and 3D Internet Agenda.

2.2.3. University of Passau

The University of Passau (UNI PASSAU) in Germany was founded in 1978. The University of Passau has been growing steadily and fast with a very strong international bias. It offers, e.g., a European Studies Programme, fosters active partnerships and exchange programmes with approximately 120 Universities world wide. In the German CHE-Ranking the computer science faculty repeatedly ranks among the top universities in Germany. A further strong characteristic of the University of Passau is the interaction between academia and industry. This will offer excellent opportunities for the dissemination of knowledge and research results both to academia, SMEs and to leading industrial partners. This has been underlined by the University winning the German Data Centre Award 2012.

Competencies: The Computer Networks and Computer Communication (CNACC) research group, headed by Prof. Hermann de Meer, is part of the Faculty of Informatics and Mathematics at the University of Passau. Main research fields are network virtualization, self-organising systems, IT security, safety, and energy-efficiency. University of Passau's research excellence has been demonstrated within numerous nationally and internationally funded projects, e.g., G-Lab_Ener-G and inSel (funded by the German Ministry of Education and Research), FIT4Green, AutoI, ResumeNet, Socionical, or All4Green (all funded by the European Union within the 7th FP). The university is a member of the EINS Network of Excellence and of the EU COST Action IC804 (Energy Efficiency in Large Scale Distributed Systems). Within some of those projects, strong ties have been built already to both Lancaster University and AIT.

Main tasks: The main tasks of the University of Passau in the HyRiM project will be focused in the area of perimeter protection enhancements. This research field offers on the one hand the opportunity to use the already present excellence of the university in this area, which was already a major focus in other projects, while on the other hand extending the knowledge into utility network facilities and infrastructures. In addition, the University of Passau will take major responsibility in the dissemination of the HyRiM results by leading and contributing to the scientific and standardisation activities.

Short profile of key people:

Prof. Hermann de Meer (http://www.fim.uni-passau.de/demeer) received his Ph.D in 1992 on the topic "Transiente Leistungsbewertung und Optimierung rekonfigurierbarer fehlertoleranter Rechensysteme". He had been an Assistant Professor at Hamburg University, Germany, a Visiting Professor at Columbia University in New York City, USA, and a Reader at University College London, UK. He is currently appointed as Full Professor at the University of Passau, Germany, and as Honorary Professor at University College London, UK. He is a Member of the Executive Board of the Institute of IT Security and Security Law (ISL) at the University of Passau. He currently holds several research grants funded by the Deutsche Forschungsgemeinschaft (DFG) and by the EU (FP6 and FP7).

Ralph Herkenhöner (http://www.net.fim.uni-passau.de/herkenhoener) is a researcher and a member of the research group of Computer Networks and Computer Communication, headed by Prof. Hermann de Meer, as well as of the Institute for IT-Security and Security Law (ISL) at the University of Passau, Germany. He is also a member of the FP7 Network of Excellence EINS, involving technology and implications of the legally compliant information security management systems. He has been working on different research projects regarding privacy and security management. Currently, he is preparing his PhD and actively investigates IT-security and data protection in communication systems, accountable and compliant IT-Security, and assessment of technical requirements from legal frameworks.

Michael Niedermeier (http://www.net.fim.uni-passau.de/mniedermeier) received his Diploma in Computer Science in 2009 from the University of Passau. Since then, he is working as a research associate at the Chair of Computer Networks and Computer Communications and at the Institute of IT Security and Security Law (ISL) at the University of Passau. His main research areas focus on energy efficient security concepts, security and functional safety in distributed systems like sensor networks or utility networks, such as the Smart Grid. Currently, he is working on the EFRE-funded SECBIT project, whose goal is to support SMEs to strengthen their IT security and safety awareness. Additionally, he is a member of the FP7 Network of Excellence EINS, which offers a platform for worldwide cooperation and interdisciplinary research of the Future Internet.

Dr. Andreas Berl (http://www.andreas-berl.de) obtained his Ph.D. at the University of Passau (Germany) in 2011. He is currently working as researcher in the Computer Networks and Communications group at the University of Passau. His research interests include virtualization, and peer-to-peer overlays. Currently he is involved in the EU project “All4Green - Active collaboration in data centre ecosystem to reduce energy consumption and GHG emissions (FP7)”. Andreas Berl is member of the EU Network of Excellence “EINS - Network of Excellence in Internet Science” and the COST Action IC0804 „Energy Efficiency in Large Scale Distributed Systems“. In 2009 he had a DAAD scholarship at Lancaster University, UK, supervised by Prof. David Hutchison.

2.2.4. ETRA Investigación y Desarrollo, S.A. (ETRA I+D)

ETRA Investigación y Desarrollo, S.A. (ETRA I+D) is the hi-tech unit within ETRA Group, one of the leading industrial groups in Spain. Its mission is putting in the market the most advanced solutions and services either directly or through the 10 companies of the Group. The main market areas of ETRA Group are Spain, South-Central America, South East Asia and the EU.
The activity of the company –with a sustained growth of turnover and employees over the years which has reached 250 M€ and 2200 staff in 2010- started in the 70's and it is centred in the RTD, implementation and commercialisation of advanced real time control and information management systems applied to the sectors of security, energy, mobility, and public services.

Competencies:
The business area of Security –considered both vertically and horizontally across the other business areas- accounts for a substantial 50% of the company turnover.
ETRA brings into the project its technological competence in the security domain, its market presence and exploitation capability, and a long success track record of managing successful EU RTD projects in the fields of ICT and SECURITY –among others-. NOBEL, BEAMS, SKYNET and PRECYSE are recent examples of large FP7 projects led by ETRA.

Main tasks:
ETRA I+D will participate in the project as leader of WP2 "Hybrid Risk Assessment for interconnected utility networks" and WP6 "Dissemination, Exploitation and Impact" and will also participate in the rest of the WPs.

Short profile of key people:

Antonio MARQUÉS holds an MSc in Physics with Computing from the University of Valencia (Spain), a Diploma in Operational Research and a Master in Business and Innovation Management. He is currently the Director of New Technologies at ETRA I+D. He has worked in the past for the DG III of the EC as Scientific Officer and at IBM. He has been involved in multinational collaborative research for seventeen years as researcher, project manager and expert working for international organisations –e.g. evaluator and reviewer for the European Commission.

Lola ALACREU is an Industrial Engineer from the Polytechnic University of Valencia (Spain), performing the last year of the degree in the Manchester University (United Kingdom). In the past she works in Carrefour Group and she is working in ETRA I+D since 2008, where has been involved in several ICT European and national projects, such as the coordination of NOBEL project.

Santiago CÁCERES is Electronic Engineer – communications networking specialization - from the Polytechnic University of Valencia (Spain). He has worked in the past in LE-Technichs (Slovenia), the Technical University of Prague (Czech Republic) and in Generalitat Valenciana (the public administration of Valencia Region, Spain). He has been involved as Project Engineer and Analyst in the New Technologies department in several EU RTD projects.

2.2.5. Akhela s.r.l

Akhela (Web: http://www.akhela.com) is a large Italian company with strong competencies and a powerful infrastructure for the development and supply of customized solutions and high quality services in two main business areas: IT services and Embedded Systems. In IT market, Akhela is focused on services and solutions for IT systems and their consolidation and performance optimization. Target customers are medium and large organisations, for which security and business continuity represent a fundamental requirement. Akhela manages the production supervision system and the information systems of one of the most important high conversion supersites in Europe, namely the Saras Refinery, located in Sarroch (Sardinia region, Italy). As a result of this activity, Akhela has developed a wealth of methodologies, competencies, experiences, procedures and systems for the supervision of mission-critical environments and services. Akhela's proven success in managing Saras and other high profile companies systems and infrastructures witnesses its ability to successfully respond to stressful and challenging requirements coming from critical situations, highly complex environments and strict schedules. The Embedded Division main markets are automotive, avionics, industrial, consumer electronics, TLC and silicon founders. For these markets Akhela programs the most demanding real time System-On-Chip Applications, with the contribution of a motivated team and in-house experts. The ownership of intellectual property rights allows Akhela's partners to benefit from highly customisable and off the- shelf, ready-to-port codes.

Competencies:

Akhela is preeminent on the security market covering the various segments of the sector. In fact Akhela experience and know-how cover physical security systems design, deployment and management (with specific regards to highly critical plants), as well as logical security services. Akhela has developed solutions in many security areas from Datacenters to industrial SCADA subsystems, from closed area protection to access control, and from IT infrastructure logical protection to application security enforcement. Akhela participates in the European project AGATA (INTERREG IIIB), DISC (Distributed Supervisory Control, FP7) TouchMore (FP7) Astute (Artemis) p+n Safecer (Artemis) Demanes (Artemis) and in several Italian (MIUR/MAP funding) research projects: FILIDIERA (e-collaboration platform), DIAGDIS (Distributed Computing Systems Diagnostics).

Main tasks:

Akhela, thanks to its experience in the security market managing framework contract with large enterprises as a customer, will be deeply involved mainly but not exclusively in the identification of the requirement of the system considering current trends of the attacks and in the definition of the different scenario that will be used as a demo of the framework and all the related activities. Furthermore some months will be spent for studying the problem related to the perimeter protection and an important task will be to drive the exploitation plan and the standardisation activities.

Short profile of key people:

Dr. Maria Katiuscia Zedda received the M.S. degree in Electrical Engineering from the University of Cagliari, Cagliari, where she received the Ph.D. degree in Industrial Engineering. During the Ph.D studies and Post-Doc experience she has been visiting researcher at JET (Joint European Torus, Culham, UK) for several years, where she was appointed for a JOC Position, secondment Agreement between European Commission, EURATOM/UKAEA, and EURATOM/ENEA in support of the experimental campaign for the plasma control and protection systems. Afterwards she has been employed in Akhela in the research and special project department.

Dr. Marco Soro received the M.S. degree in Electrical Engineering from the University of Cagliari. After a short experience as researcher, he has been employed in Akhela where he worked in the field of modelling and simulation of dynamic systems, real time systems for automotive, calibration protocols and diagnostic system. In the last 4 years he is working in the Oil & Gas division, where he has been appointed as supervisor and responsible of several projects related to security issues of the refinery and critical infrastructure.

Carla Cannas is an experienced Quality Manager; she has a degree in Foreign Languages and Foreign Literatures and has been working in Akhela since 1998. Latest experience was as Project Manager for ERP systems development and maintenance projects. Currently she is in charge of the implementation of standards and best practices in software development processes.

2.2.6. Suministros Especiales Alginetenses, Coop. V.

Cooperativa Electrica de Alginet (Electrical co-operative of Alginet) is an electrical energy supplier installed in Alginet (Valencia – Spain) in the year 1930. Nowadays, it supplies 45 million Kilowatts per year (5.700 consumers) with 18.000 Kilowatts installed power capacity thanks to 35 transformation centres. A new electrical energy substation has being built, with 40Megawatts to guarantee the current and future energy demand in the whole town. The substation, with a budget for the implementation of more than 3.5 million euros, will be of exclusive use of the cooperative. Initially it doubles the available power, but in long term, it quadruples this power. With the construction of the new facility, the electric cooperative of Alginet is the first cooperative that manages a substation in property.
Additionally, a pioneer system of smartmetering has being implemented in the electric cooperative of Alginet. The consumption of each user can be metered automatically via these smartmeters. Alginet is the first municipality in Spain implementing a smartgrid, based on a technology called PLC - Power Line communications-. Another advantage is that the periodicity of the data collection, that could be weekly, daily or even every 15 minutes, can be programmed. By means of these smartmeters the estimated readings and errors could be avoided.

Competencies:
The electric cooperative of Alginet, being a non-profit organisation, will protect their own infrastructures and equipment of different attacks offering better services to their clients.

Main tasks:
Suministros Especiales Alginetenses, Coop. V. will participate in the project mainly as end-user, contributing to the requirements specification and as a pilot site in order to demonstrate the project results in its own facilities.

Short profile of key people:

José Vicente ORTUÑO SOLER, General Manager. Vicente received a High degree in electronics and computer sciences from the Polytechnic University of Valencia (Spain). Vicente also holds a Master's degree in cooperatives managing at the University of Florida (Valencia). Vicente has been working in the Electrical cooperative of Alginet from 1979, first in the administration department and currently as general manager.

Rafael ALEMANY BIVIA, Technical manager. Rafael is Industrial Engineer from the Polytechnic University of Valencia (Spain). As previous experiences, Rafael has worked as engineer in several companies such as ICESSA and MERLIN GERIN and currently he is technical manager of the Electrical cooperative of Alginet from 2001.

2.2.7. Linz AG

LINZ AG für Energie, Telekommunikation, Verkehr und kommunale Dienste (Engl. Linz AG for Energy, Telecommunications, Public Transport, and Community Services)

LINZ AG is run as an Austrian management-holding with four operative multi utility subsidiaries and with one Service Company for the city of Linz and parts of Upper Austria. A contemporary, market-oriented corporation was developed, in order to conserve costs and to secure profits through the exhaust of synergy-potentials. In addition, the foundation for the future orientation as a "multi-utility supplier" was created. The corporate structure contains the following entities:

- The LINZ AG for Energy, Telecommunications, Public Transport, and Community Services LTD is run as an active management-holding with four operative subsidiaries and with one service subsidiary.
- LINZ STROM GmbH for Power Generation, Trade, Services and Telecommunications is responsible for the fields of energy production and distribution, for sales, and for telecommunications.
- LINZ GAS/WÄRME GmbH for Natural Gas and for the Supply of Heat is responsible for the supply of gas, district heating, and for the provision of installation services.
- LINZ LINIEN GmbH for Local Transport is responsible for all areas of local transport.
- LINZ SERVICE GmbH for Infrastructure and Community Services is responsible for the infrastructure supply with water, the disposal of waste water and refuse, community services, such as the harbor, public pools as well as funerals and cemeteries.

K. Rossegger
Mr. Karl Rossegger has a Master Degree in Telecommunication and Computer Science from the Technical University of Graz, Austria**.** From 1989 to 1994, he did Computer science trainings and consulting for data management systems. Since 1997, he has been project manager for telecommunication in LINZ AG. In 1999 he joined the department of “Telecommunication Technology” of LINZ AG as project manager for internet and communication technology and since 2002 he is head of the department with 66 employees.

B. Haberler
Mr. Berthold Haberler has also a Master Degree in Telecommunication and Computer Science from the Technical University of Graz, Austria. From 2001 to 2006 he was working as an engineer both in chip design for RFID chips (Radio Frequency IDentification) but later on also as project manager for design and development of RFID systems including selection of technology and components as well as specification of software. In this function he was able to gain experince in communication engineering, system specification and implementation, as well as project management. Since October 2006 he is with LINZ AG, working as project & innovation manager in the field of research and system enhancement projects.

2.3. Consortium as a whole

The HyRiM consortium is composed of a balanced international team of complementary organisations including multi-utility providers, industrial partners, research centres and universities, all of them with strong experience in the fields of risk management, security architectures and/or surveillance technologies in the context of (multi) utility provision.
Three consortium members represent end-users, i.e. utility provider, viewpoints. These are Akhela (Italy) which operates the utility control networks of an Italian refinery, Linz AG which provides multiple utilities in the area of upper Austria, and the Electrical Cooperative of Alginet which is a regional electricity provider near Valencia in Spain. Thus we are able to make reality checks of our approaches from the start, and throughout the project duration.

Each organisation provides its unique expertise: research centres and universities contribute with their analysis, methodological, dissemination support and development work; the industrial companies bring into the consortium their knowledge and leadership in the security area, secure software architectures and technological development; and finally, utility providers bring their unique expertise and knowledge in managing critical infrastructures, identifying threats and risks as well as extracting their concrete requirements in the area of cyber security in CI. In combination, all of these partners make the HyRiM approach feasible and effective.

The consortium comprises 7 partners from 5 different EU countries: two utility operators, two industry companies, two universities and a research centre. This international links are important as they represent the current situations of utility providers which are increasingly interlinked with each other to satisfy the growing demands of the free market.

Figure 5: HyRiM Consortium on the European landscape

2.3.1. Sub-contracting

Subcontracting is foreseen only for the production of Certificate of Financial Statement (CFS), for the payment of the external experts from the ELAB, and for payment in connection with hosting dissemination events. Financial resources for the production of CFS have been reserved for the following 4 beneficiaries: AIT, UNI PASSAU, ULANC and ETRA. A total amount of € 15.909 has been reserved for the experts from the ELAB (cf. Table 9 and Table 10). For hosting dissemination events, the print of brochures, and for the establishment of a project website € 24,500 have been estimated, with € 20,000 for the coordinator and € 4,500 for LINZ.

2.3.2. The HyRiM Advisory Board

Additionally to the consortium partners themselves, the HyRiM project will build an extended Advisory Board, consisting of several organisations that are interested in the research results of the project. A goal of the project is to increase this Advisory Board during the course of the project, as part of our dissemination activities.

The Austrian multi-utility providers

- Energie AG Oberösterreich Data GmbH (ENAG)
- Energie Versorgung Niederösterreich – EVN

have already expressed their interest in our new approaches to hybrid risk assessment, guidelines, reference architectures and surveillance technology enhancements.
Other international institutions and companies interested in the HyRiM project are

- ENDESA
- Iberdrola
- Red Eléctrica de España
- Electric cooperative of Alginet
- Electric cooperatives federation
- ASEME (Association of Electric Companies)
- GEODE (Groupement Européen des entreprises et organismes de Distribution d'Energie)

We will consult them with regard to their requirements for our approaches. They will be invited to Advisory Board meetings and we intend to leverage this link to get more utility providers on board. Additionally, we intend to invite some regulation and standardisation organisations that we plan to inform about our research outputs, including national standardisation bodies, and ENISA (European Network and Information Security Agency).

The number of companies in the HyRiM Advisory Board is not fixed yet; moreover, we will try to attract more companies from all over Europe during the initial phase of the project to bring a larger variety of requirements and practical knowledge into the HyRiM project. This will make the models and algorithms developed throughout the HyRiM project more suitable to different fields of application.

2.4. Resources to be committed

The following table illustrates the breakdown of PMs of the whole HyRiM project.

WP	Title	Resources (PM)	Percentage
WP 1	Hybrid Risk Metrics and Methodology for Risk Assessment	99	22.5%
WP 2	Hybrid Risk Assessment for Interconnected Utility Networks	78	17.7%
WP 3	Human and Organisational Risk Analysis	44	10.0%
WP 4	Perimeter Protection Enhancements	66	15.0%
WP 5	Evaluation and Assessment of Project Results in Simulated and Real Testbed Environments	72	16.4%
WP 6	Dissemination, Exploitation and Impact	50	11.4%
WP 7	Project Management	31	7.0%
	Total	440	100%

Table 7: Resources breakdown per WP

Here it is a detail on the total requested budget, broken down on its main components (all costs are stated in Euros):

	AIT	ULANC	UNI PASSAU	ETRA	AKH	ECA	LINZ	Total
PM	**95**	**63**	**80**	**86**	**67**	**27**	**22**	**440**
Personnel costs	698,488	369,306	468,560	494,500	351,750	162,000	150,920	2,695,524
Equipment costs	0	0	3,000	0	20,000	0.00	2,500	25,500
Travel costs	* 111,600	46,800	46,800	30,600	30,600	30,600	30,600	327,600
Other direct costs	0	0	6,000	0	0	0	0	6,000
Indirect costs	494,034	249,664	314,616	247,250	80,470	115,560	45,276	1,546,870
Subcontracting costs	27,500	5,685	** 15,909	2,500	0	0	4,500	56,094
Budget	**1,331,622**	**671,455**	**854,885**	**774,850**	**482,820**	**308,160**	**233,796**	**4,657,588**
Funding	**1,136,129**	**512,211**	**657,082**	**454,449**	**279,390**	**205,440**	**142,384**	**3,387,085**

(* including budget for Advisory Board, ** including budget for ELAB)

Table 8: Budget breakdown by concept

Here is a detailed budget breakdown per beneficiary for each category of foreseen expenses:

Partner Number	Partner Name	RTD							
		Personnel	Subcontr.	Other direct costs				Indirect Costs	Total
				Consumable	Travel	Equipment	Meetings		
1	AIT	€ 411.740,00			€ 10.800,00			€ 291.220,00	€ 713.760,00
2	UNI PASSAU	€ 380.705,00			€ 10.800,00	€ 3.000,00		€ 236.703,00	€ 631.208,00
3	ULANC	€ 310.686,00			€ 10.800,00			€ 192.892,00	€ 514.378,00
4	ETRA	€ 316.250,00			€ 10.800,00			€ 158.125,00	€ 485.175,00
5	AKH	€ 189.000,00			€ 10.800,00	€ 15.000,00		€ 42.960,00	€ 257.760,00
6	ECA	€ 60.000,00			€ 10.800,00			€ 42.480,00	€ 113.280,00
7	LINZ	€ 82.320,00			€ 10.800,00			€ 24.696,00	€ 117.816,00
									€ 2.833.377,00

Partner Number	Partner Name	DEMO							
		Personnel	Subcontr.	Other direct costs				Indirect Costs	Total
				Consumable	Travel	Equipment	Meetings		
1	AIT	€ 14.705,00			€ 9.000,00			€ 10.401,00	€ 34.106,00
2	UNI PASSAU	€ 40.999,00			€ 9.000,00			€ 29.999,00	€ 79.998,00
3	ULANC	€ 29.310,00			€ 9.000,00			€ 22.986,00	€ 61.296,00
4	ETRA	€ 97.750,00			€ 9.000,00			€ 48.875,00	€ 155.625,00
5	AKH	€ 110.250,00			€ 9.000,00	€ 5.000,00		€ 24.850,00	€ 149.100,00
6	ECA	€ 84.000,00			€ 9.000,00			€ 55.800,00	€ 148.800,00
7	LINZ	€ 41.160,00			€ 9.000,00	€ 2.500,00		€ 12.348,00	€ 65.008,00
									€ 693.933,00

Partner Number	Partner Name	MGMT							
		Personnel	Subcontr.	Other direct costs				Indirect Costs	Total
				Consumable	Travel	Equipment	Meetings		
1	AIT	€ 169.108,00	€ 7.500,00		€ 64.800,00			€ 119.608,00	€ 361.016,00
2	UNI PASSAU	€ 29.285,00	€ 15.909,00		€ 6.000,00			€ 21.171,00	€ 72.365,00
3	ULANC		€ 5.685,00						€ 5.685,00
4	ETRA		€ 2.500,00						€ 2.500,00
5	AKH	€ 15.750,00						€ 3.150,00	€ 18.900,00
6	ECA								€ 0,00
7	LINZ								€ 0,00
									€ 460.466,00

Partner Number	Partner Name	OTHER							
		Personnel	Subcontr.	Other direct costs				Indirect Costs	Total
				Consumable	Travel	Equipment	Meetings		
1	AIT	€ 102.935,00	€ 20.000,00		€ 27.000,00			€ 72.805,00	€ 222.740,00
2	UNI PASSAU	€ 17.571,00			€ 27.000,00			€ 26.743,00	€ 71.314,00
3	ULANC	€ 29.310,00			€ 27.000,00			€ 33.786,00	€ 90.096,00
4	ETRA	€ 80.500,00			€ 10.800,00			€ 40.250,00	€ 131.550,00
5	AKH	€ 36.750,00			€ 10.800,00			€ 9.510,00	€ 57.060,00
6	ECA	€ 18.000,00			€ 10.800,00			€ 17.280,00	€ 46.080,00
7	LINZ	€ 27.440,00	€ 4.500,00		€ 10.800,00			€ 8.232,00	€ 50.972,00
									€ 669.812,00

Table 9: Budget breakdown by category

Personnel costs. As shown in A3 form, the partners have been allocated resources according to their real personnel costs as stipulated by their respective cost models.

Special considerations should also be made about **Project Management costs (WP7)**, which do not exceed 7% of total person month effort.

Management costs. In order to avoid overloading the management budget, the resources covering auditing costs of each partner have been included in the budget allocation. Costs have been estimated to € 2,500 per audit certificate for AIT and ETRA, and to € 5,685 for ULANC. It is worth to mention that UNI PASSAU makes use of a competent public officer to provide the required audit certificates. These audit costs of € 6,000 are stated in the other direct costs of UNI PASSAU.

Travel costs. The project will require several regular meetings for good co-operation and integration. Travel budget is about 7% of total budget allocated, including € 54,000 for Advisory Board expenses as mentioned in Table 10 in the budget of the coordinator. The distribution of travel expenses has been performed uniformly according to the involvement of each project partner.

Workshop	Number of Advisory Board members requiring expenses	Average travel costs per expert	Costs
WS 1	10	900	9,000
WS 2	20	900	18,000
WS 3	30	900	27,000
		Total costs for HyRiM Advisory Board	54,000

Table 10: Costs of Advisory Board

All the partners will attend two plenary meetings per year (when possible, coinciding with the scientific and technical dissemination activities of the project), as well as a kick-off meeting and a final project meeting. These Meetings will be hosted by each of the partners such that travel efforts are balanced among all partners. In detail, the kick-off meetings and the final project meeting will be held in Vienna, two plenary meetings in Passau and one meeting in Lancaster, Valencia and Cagliary, respectively. Additionally, there are two project review meetings in Brussels where representatives of each partner will attend. A detailed description of all travel costs can be found in Table 11.
In addition, all partners will have to travel in order to cooperate in the demonstration actions of WP5. Here, the location of the meetings is distributed between Italy (hosted by AKH) and Spain (hosted by ECA), since AKH and ECA are the two members of the consortium, who are mainly responsible for the demonstration.
Regarding dissemination activities three workshops with utility providers and policy makers as well as legislation and standardization bodies are planned. During these workshops the requirements will be provided and the impact of the outcomes of the project will be assessed. Additionally, the end users involved in these workshops will give relevant feedback to refine the project results. The workshops will be hosted by the coordinator (AIT) at Vienna, they will last between two and three days and they will involve end users from all partner states. We will target a broad community but at this time it is not clear which institutions will be invited to participate in these workshops. The first two workshops are scheduled to be held at the middle of the project during year 2, when first results are available. The final workshop will be held towards the end of the project to present the final results to a broad community of utility providers, policy makers and standardisation bodies.
In addition to these workshops, five conference visits per project for the academic partners (AIT, ULANC, UNI PASSAU) and two visits per year for the industry partners have been estimated as dissemination activities. The project coordinator requires further travel budget for networking and project representation.

				AIT			ULANC			UNI PASSAU			ETRA			AKH			ECA			LINZ		
Meeting	**Date**	**Host**	**Location**	**#**	**Cost**	**Total**	**#**	**Cost**	**Total**	**#**	**Cost**	**Total**	**#**	**Cost**	**Total**	**#**	**Cost**	**Total**	**#**	**Cost**	**Total**	**#**	**Cost**	**Total**
RTD																								
Kick-Off Meeting	Jan-14	AIT	Vienna	2	€ 0	€ 0	2	€ 900	€ 1.800	3	€ 260	€ 780	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 450	€ 900
Plenary Meeting 1	Jul-14	UNI PASSAU	Passau	2	€ 900	€ 1.800	2	€ 900	€ 1.800	3	€ 0	€ 0	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 900	€ 900
Plenary Meeting 2	Jan-15	ULANC	Lancaster	2	€ 900	€ 1.800	2	€ 0	€ 0	3	€ 754	€ 2.262	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 900	€ 900	2	€ 900	€ 1.800
Plenary Meeting 3	Jul-15	ETRA	Valencia	2	€ 900	€ 1.800	2	€ 900	€ 1.800	3	€ 720	€ 2.160	2	€ 0	€ 0	2	€ 900	€ 1.800	2	€ 0	€ 0	1	€ 900	€ 900
Plenary Meeting 4	Jan-16	AKH	Cagliari	2	€ 900	€ 1.800	1	€ 900	€ 900	3	€ 668	€ 2.004	2	€ 900	€ 1.800	2	€ 0	€ 0	2	€ 900	€ 1.800	2	€ 900	€ 1.800
Plenary Meeting 5	Jul-16	UNI PASSAU	Passau	2	€ 900	€ 1.800	1	€ 900	€ 900	3	€ 0	€ 0	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800
Final Project Meeting	Nov-16	AIT	Vienna	2	€ 0	€ 0	2	€ 900	€ 1.800	3	€ 260	€ 780	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 450	€ 900
Review Meeting 1	Jul-15	EU	Brussels	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 938	€ 938	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 900	€ 900
Review Meeting 2	Dec-16	EU	Brussels	1	€ 900	€ 900	1	€ 900	€ 900	2	€ 938	€ 1.876	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 900	€ 900	1	€ 900	€ 900
DEMO																								
WP 5 Demo Meeting	Oct-15	AKH	Cagliari	2	€ 900	€ 1.800	2	€ 900	€ 1.800	3	€ 668	€ 2.004	3	€ 900	€ 2.700	3	€ 0	€ 0	3	€ 900	€ 2.700	2	€ 900	€ 1.800
Demo Prep. 1	Jan-16	AKH	Cagliari	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 669	€ 1.338	3	€ 900	€ 2.700	3	€ 0	€ 0	3	€ 900	€ 2.700	2	€ 900	€ 1.800
Demo Prep. 2	Jul-16	ECA	Valencia	2	€ 900	€ 1.800	2	€ 900	€ 1.800	3	€ 720	€ 2.160	4	€ 0	€ 0	5	€ 900	€ 4.500	4	€ 0	€ 0	2	€ 900	€ 1.800
Demo Prep. 3	Sept-16	AKH	Cagliari	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 669	€ 1.338	4	€ 900	€ 3.600	3	€ 0	€ 0	4	€ 900	€ 3.600	2	€ 900	€ 1.800
Final Project Demo	Oct-16	ECA	Valencia	2	€ 900	€ 1.800	2	€ 900	€ 1.800	3	€ 720	€ 2.160	4	€ 0	€ 0	5	€ 900	€ 4.500	4	€ 0	€ 0	2	€ 900	€ 1.800
MGMT																								
User Group Workshops		N/A	TBD	60	€ 900	€ 54.000																		
Management Travel	see above					€ 10.800																		
OTHER																								
Diss. Workshop 1		AIT	Vienna	2	€ 0	€ 0	2	€ 900	€ 1.800	3	€ 260	€ 780	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800
Diss. Workshop 2		AIT	Vienna	2	€ 0	€ 0	2	€ 900	€ 1.800	3	€ 260	€ 780	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800
Diss. Workshop 3		AIT	Vienna	2	€ 0	€ 0	2	€ 900	€ 1.800	3	€ 260	€ 780	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800	2	€ 900	€ 1.800
Acad. Dissemination		N/A	TBD	3	€ 1.800	€ 5.400	2	€ 1.800	€ 3.600	14	€ 1.212	€ 16.968												
Acad. Dissemination		N/A	TBD	3	€ 1.800	€ 5.400	2	€ 1.800	€ 3.600	3	€ 2.564	€ 7.692												
Acad. Dissemination		N/A	TBD	3	€ 1.800	€ 5.400	2	€ 1.800	€ 3.600															
Acad. Dissemination		N/A	TBD	3	€ 1.800	€ 5.400	3	€ 1.800	€ 5.400															
Acad. Dissemination		N/A	TBD	3	€ 1.800	€ 5.400	3	€ 1.800	€ 5.400															
Indust. Dissemination		N/A	TBD										1	€ 1.800	€ 1.800	3	€ 900	€ 2.700	1	€ 1.800	€ 1.800	1	€ 1.800	€ 1.800
Indust. Dissemination		N/A	TBD										2	€ 1.800	€ 3.600	3	€ 900	€ 2.700	2	€ 1.800	€ 3.600	2	€ 1.800	€ 3.600
						€ 111.600			€ 46.800			€ 46.800			€ 30.600			€ 30.600			€ 30.600			€ 30.600

Table 11: Travel Cost Breakdown

Equipment costs. The RTD equipment costs for AKH split up into 4 laptops used for development during the entire project runtime as well as a HR monitor, a dedicated server and cable and small parts (cf. Table 12 for details). For the DEMO, a SCADA kit is required. The RTD equipment costs for UNI PASSAU split up into 3 smartphones and respective SIM-cards to operate in 3 different countries (Germany, Italy and Spain) as well as a sensor network used as testbed for on-demand (cf. Table 12 for details).

RTD - UNI PASSAU			
Item	**Price per Item**	**No. Of Items**	**Cost**
Nexus4 16GB	325,00 €	3	975,00 €
Simcards (including data traffic)	50,00 €	9	450,00 €
ConnectPort X2e ZigBee SE Router, Ethernet and Wi-Fi	75,00 €	1	75,00 €
iSense node	500,00 €	3	1.500,00 €
			3.000,00 €
RTD - AHK			
Item	**Price per Item**	**No. Of Items**	**Cost**
Development Laptop	€ 1.875,00	4	€ 7.500,00
Development Server	€ 5.000,00	1	€ 5.000,00
HR monitor	€ 2.000,00	1	€ 2.000,00
Cable and small parts	€ 500,00	1	€ 500,00
			15.000,00 €
DEMO - AHK			
Item	**Price per Item**	**No. Of Items**	**Cost**
SCADA development kit	€ 5.000,00	1	€ 5.000,00
			€ 5.000,00

Table 12: Equipment Cost Breakdown

Other costs. For hosting dissemination events, the print of brochures, and for the establishment of a project website € 24,500 have been estimated and stated as other subcontracting costs for the project coordinator with € 20,000 and for LINZ with € 4,500.

Indirect costs. This amount corresponds to the overheads of each partner, depending on the cost model used in their accounting system to keep track of such costs. The following table, extracted from the A3 forms, summarises the main cost per activity type.

	RTD	**DEMO**	**MGM**	**OTHER**	**Total**	**Percentage**
Personnel	1,750,701	418,174	214,143	312,506	2,695,524	57.87%
Subcontracting	0	0	31,594	24,500	56,094	1.21%
Other direct costs	93,600	70,500	70,800	124,200	359,100	7.71%
Indirect costs	989,076	205,259	143,929	208,606	1,546,870	33.21%
TOTAL	2,833,377	693,933	460,466	669,812	4,657,588	100%
Percentage	60.83%	14.90%	9.89%	14.38%	100%	
Requested EC funding	1,909,843	346,966	460,465	669,811	3,387,085	

Table 13: A3 Form summary

			Lead	Contr.	AIT	ULANC	UNI PASSAU	ETRA	AKH	ECA	LINZ	Total
WP1	**Hybrid Risk Metrics and Methodology for Risk Assessment**				**25**	**12**	**17**	**20**	**9**	**10**	**6**	**99**
	T 1.1	Trend analysis of (cyber) risk on utility networks	ULANC		1	6	9	4	3	7	4	**34**
	T 1.2	Deriving requirements from utility providers	ETRA			3		8	4		2	**17**
	T 1.3	Definition of hybrid risk metrics and assessment methods	AIT		24		5	4				**33**
	T 1.4	Categorisation of vulnerabilities based on Hybrid Risk Metrics	ETRA			3	3	4	2	3		**15**
WP 2	**Hybrid Risk Assessment for Interconnected Utility Networks**				**20**	**15**	**7**	**25**	**9**	**0**	**2**	**78**
	T 2.1	Identification of SCADA-related attack characteristics as wells as mitigation and	ETRA		6	6	7	14	2		2	**37**
	T 2.2	Definition of a Hybrid Risk Metric in SCADA attack scenarios	AIT		8	3		5	2			**18**
	T 2.3	Provision of tools for Hybrid Risk Management in SCADA networks based on existi	AKH		6	3		3	5			**17**
	T 2.4	Application of Hybrid Risk Metrics in defence measures such as preventative poli	ULANC			3		3				**6**
WP 3	**Human and Oragnisational Risk Analysis**				**5**	**21**	**6**	**10**	**0**	**0**	**2**	**44**
	T 3.1	Investigation of organizational factors within utility organizations	ULANC		1	5					2	**8**
	T 3.2	Investigation of incidents using secondary data	ULANC			5	2					**7**
	T 3.3	Investigation of risk responses in society	ULANC			5	2					**7**
	T 3.4	Development of analytical framework and metrics	ULANC			6	2	4				**12**
	T 3.5	Development of monitoring approaches and a reference framework	ETRA		4			6				**10**
WP 4	**Perimeter Protection Enhancements**				**6**	**5**	**35**	**0**	**18**	**0**	**2**	**66**
	T 4.1	Surveillance Technologies Trend Analysis	ULANC			5	8		3		2	**18**
	T 4.2	Dealing with threats by surveillance	AKH				4		3			**7**
	T 4.3	Application of surveillance to compute Hybrid Risk Metrics	UPASS				5		3			**8**
	T 4.4	Application of Hybrid Risk Metrics and Assessment to support surveillance	UPASS		3		4		4			**11**
	T 4.5	On-Demand Surveillance Enhancement	UPASS		3		14		5			**22**
WP 5	**Evaluation and Assessment of Project Results in Simulated and Real Testbed Environments**				**2**	**5**	**7**	**17**	**21**	**14**	**6**	**72**
	T 5.1	Identification and involvement of end-users	AKH		2	5		4	12	7	6	**36**
	T 5.2	Definition of use cases	AKH					4	6			**10**
	T 5.3	Surveys with regards to user acceptance	ECA					3		4		**7**
	T 5.4	Survey with utility providers	ECA					2	3	3		**8**
	T 5.5	Evaluation, preparation and presentation of results for policy and decision make	UPASS				7	4				**11**
WP 6	**Dissemination, Exploitation and Impact**				**14**	**5**	**3**	**14**	**7**	**3**	**4**	**50**
	T 6.1	Workshop with utility providers and policy makers	AIT		6			3	1	1	2	**13**
	T 6.2	Dissemination Activities	UPASS		4	4	2	3	1	1	1	**16**
	T 6.3	Liaison, standardisation and regulation activities	ETRA		2			4	2			**8**
	T 6.4	Exploitation Plan	AKH		2	1	1	4	3	1	1	**13**
WP 7	**Project Management**				**23**	**0**	**5**	**0**	**3**	**0**	**0**	**31**
	T 7.1	Legal and Financial Management	AIT		13							**13**
	T 7.2	Management of Project Execution	AIT		10				3			**13**
	T7.3	Management of Legal, Ethical, Privacy and Policy Issues	AIT				5					**5**
Total PM					**95,0**	**63,0**	**80,0**	**86,0**	**67,0**	**27,0**	**22,0**	**440,0**

Table 14: person months related to tasks

For more detailed information per partner, please refer to A3 forms.

3. Impact

3.1. Expected impacts listed in the work programme

3.1.1. Overall impact

We envisage the main impact of the HyRiM project as a significant increase in awareness of the utility providers towards cyber security, resilience, and the human factor as a major problem in their infrastructures. HyRiM will provide utility providers with new ways of assessing the risk in their interconnected structure of control and utility networks. We assess current and future cyber risks (e.g., Advanced Persistent Threats (APT) or Denial of Service (DoS)) in SCADA systems and the interplay and propagation of threats inside interconnected utility networks. Additionally, we incorporate novel surveillance technologies to increase the security of the extended perimeter of utility providers and the human factor as a potential source of threats (for example by personally owned digital/communication devices used in business day to day life). These concrete examples will be used as a source for quantitative measures backed by mathematically proven models, which will help both stakeholders and consumers to increase their understanding and allow the evaluation of risks in utility networks.

3.1.2. Expected impacts listed in the work programme

Impact 1: Operators of utility networks, which represent a critical infrastructure, are expected to gain a better understanding of risks against their own infrastructures.

Utility networks can be considered as critical and fragile supportive structures of the society. Risk awareness rests on a comprehensive insight into the system, which is normally infeasible due to complexity and for security reasons. Consequently, policy makers and stakeholders are often confronted with vague (fuzzy) facts related to system aspects, especially when it comes to (cyber) risk and threats. The project will develop a method to abstract from technical details of a system so as to leave a stakeholder (whether this is a decision- or policy maker or an arbitrary customer) with qualitative and/or quantitative indicators related to security under current and potential future (cyber) attacks. After all, decisions to use, extend, improve, refrain from using or even perhaps to destruct a utility network must rest on sound facts with unambiguous interpretations. Hybrid risk measures will be designed to support this by quantifying security in a network in terms of multiple indicators that explicitly account for mutual interplay and directly relate to every part of the overall system that is critical. More importantly, an assessment in this form allows comparison of different utility network designs in terms of common performance indicators. Based on these indicators, the level of criticality of certain parts of a utility network or the utility network as a whole can be classified and provider companies but also the legislation can create guidelines based on standards that rely on the general method.

Impact 2: Explicit static and dynamical models to categorise different types of utility networks allow to study security risks, manifestations of vulnerabilities and to simulate impacts of changes/improvements.

The costs associated with applying security measures are evident, but the potential benefits are much harder to measure. This can lead to poor uptake of security measures, in general, and particularly in utility networks, in which issues of (cyber) security have traditionally been focused on availability of the infrastructure and resilience to faults and environmental effects. Especially with the rise of interconnected SCADA systems, such as Smart Grid technology, manufacturers and providers of utility networks must be supplied with simulation models for decision making towards maximal security and safety. While these are two different sides of the same medal already, hybrid risk measures offer a much broader and holistic view on a utility network being a compound of several networks with potentially complex interdependencies. Alongside with the scientific output of the project, we will deliver business cases and show how hybrid risk measures and simulation models can be used for quantitative risk management and decision making throughout the whole

life-cycle of a utility network. The theoretical results will be supported by real-life experimental validations carried out in the course of WP5.

Impact 3: Input on global guidelines for critical infrastructures based on a multi-dimensional understanding of the interplay of connected SCADA systems, human factor, and surveillance; in particular new innovative methodologies minimising the cyber risks and threats to these systems.

The research activities carried out on the project will have impact with respect these concerns in the following ways: building on real-life use cases derived from stakeholder engagement, the vulnerability of utility networks to future (cyber-)threats will be evaluated using novel techniques developed in the project. This evaluation is a key component of the risk assessment activity in the project. Explicit attention is paid to the human factor in WP3, especially to understand how vulnerabilities via human failure or insider attacks evolve and can be prevented. Besides, we will deliver novel techniques of surveillance to get early warnings about intrusions or potential information leakage (e.g., control information that allows hitting the network at a neuralgic point or in a neuralgic state for a denial of service). The outcomes from this vulnerability analysis will be fed back to stakeholders and, as mentioned earlier, can be used to prioritise and shape new security standards and technology for utility networks. The project will develop novel technologies in important areas for utility networks, such as resilient (technical) control systems and organisational models; vulnerability manifestation and evolution, and system vulnerability and threat monitoring. As a consortium we propose development in these areas as being needed as a high priority that will have significant impact on the safety and security of utility networks. The precise nature of the design and implementation of these technologies will be supported by stakeholder engagement.

Impact 4: Developing novel quality risk assessment techniques and tools increasing the understanding of utility networks, supporting standardisation and legislation activities.

The demonstration activities encapsulated in WP5 will serve as a showcase to convince potential Advisory Board members of the feasibility of the method. More importantly, the theoretical considerations will be open to customizable risk assessment taxonomies to be used with the risk assessment techniques. The benefit of this is twofold: 1) Thanks to the theoretical construction, the units in which the hybrid risk measures (indicators) are delivered are the same as used for the network modelling. Hence, communicability and interoperability of utility network models and risks derived from them is assured at all stages. 2) For legislation, this opens the possibility to define (or re-use existing) standard taxonomies and techniques for risk assessment with the hybrid risk assessment approach. To optimally support such standardisation, interviews with stakeholders carried out throughout several work packages in the project will provide input to design the standard to achieve maximal user acceptance and compliance to requirements of utility network providers and manufacturers.

Impact 5: Improvement of theoretical and practical understanding of utility network infrastructures paving way towards automated and optimized utility network design.

Hybrid risk measures come as performance indicators related to several aspects of the network under consideration. From the viewpoint of a provider running and existing network infrastructure, these can easily be taken as pointers towards where to improve or extend the network to achieve better quality of service (quality of security/safety). If a network is designed from scratch, hybrid risk measures can be plugged into optimization procedures (software) that allows for optimized designs to be computed in a partially automated manner. The project will provide the theoretical background and fundament so that future research in the direction of optimized network design or

network optimization can build upon a solid fundament. Thanks to future threat predictions delivered in WP1, WP2 and WP4, such optimizations can even account for potential future scenarios.

3.1.3. Impact at European level

There are several key European bodies that deal directly or indirectly with the security and safety of critical infrastructures such as utility networks. The most noticeable among them are:

- the European Network and Information Security Agency (ENISA), which acts as a hub for exchange of information, best practice and knowledge in the field of information security,
- the European Public-Private Partnership for Resilience (EP3R), which is a Europe-wide governance framework for the resilience of ICT infrastructures. Its goal is to foste cooperation between the public and private sectors on security and resilience policy issues,
- the EU initiative on Critical Information Infrastructure Protection (CIIP) aims to protect Europe from large scale cyber-attacks and cyber disruptions by enhancing preparedness, security and resilience in vital Information and Communication Technology (ICT) infrastructures[83].

The Commission has requested ENISA to develop a trusted partnership with member states and stakeholders to devise an appropriate data collection framework, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence. Risk management is one of their core interests and respective guidelines and inventories for methods, tools and best practices have been collected and installed. Additionally to risk management, ENISA has a large group focused on Critical Information Infrastructure Protection (CIIP) which the security of Industrial Control Systems (ICS), including SCADA networks, as one of their main topics. Here, ENISA deals in particular with raising awareness of infrastructure operators as well as standardisation and public bodies. In parallel, they try to provide a deeper insight into this issue by engaging academia, R&D and ICS security tools and service providers. HyRiM will support and facilitate some of the intentions for a European network of security information exchanges by contributing and sharing methodologies, technologies, and best practise for risk assessment and risk management in the sensitive field of utility providers. Since the methodologies, frameworks and tools developed in the HyRiM project are coming from up-to-date research many of the HyRiM results will enhance the ENISA security and risk management guidelines and complement them with specific concepts and tools. One special focus of the ENISA lies within the field of emerging and future risks where the HyRiM results regarding cascading effects in interconnected networks may give new insights for this work group. Since the security and risk assessment in SCADA networks is a major part of this project, HyRiM aims to support the CIIP work group with new insights into threats and countermeasures

The five pillars stated by the CIIP group will therefore be used as a guideline for the expected impact of the HyRiM project on a European level.

Pillar 1: Human and technical preparedness of stakeholders and incident prevention

As a first level, the results of the HyRiM project will help utility providers by investigating and classifying surveillance technologies, which can then be used to proactively reduce risks before incidents can happen. To do so, future trends in surveillance methods are investigated and novel solutions are proposed to enhance the current possibilities. To further improve the preparedness of utility providers, novel methodologies to model (cyber) risks will be developed to identify and react to states that potentially lead to risks. The solutions will thereby not just react after an incident has already occurred, but already during the development of the risk over time. In combination with one of the main outcomes of the project – the Hybrid Risk Metrics – this gives utility providers a solid

[83] In particular, this addresses SCADA security (cf. BSI “Recommendations for critical information infrastructure protection”, https://www.bsi.bund.de/ContentBSI/EN/Topics/Criticalinfrastructures/recommend.html

foundation to better understand and prevent both current and future risks in interconnected utility networks.

Pillar 2: Detection of and response to cyber threats and incidents in utility networks

As a second pillar, the detection and response to an incident is of critical importance. Here, HyRiM can enhance the current situation in two ways: First, the novel surveillance technologies and approaches that will be developed during the project can detect incidents at both a utility and network level. This can be achieved by utilizing on-demand surveillance systems which can be used the increase the surveillance capabilities over current systems. Second, an enhanced interaction between human operators and control systems is achieved by the HyRiM Hybrid Risk Metrics. These enable to evaluate the most suited reaction to a certain event. In addition, by gaining a better understanding of the effectiveness of the response management in certain situations, the behavior of human operators can be enhanced to effectively respond to incidents.

Pillar 3: Mitigation of impact and recovery from threats and incidents in utility networks

Threats and incidents may not only cause failure of utility networks but also can affect the surveillance and control infrastructure. Therefore, HyRiM investigates and develop novel on-demand surveillance technologies (e.g., the integration of personally owned electronic devices in surveillance infrastructures) to compensate for impaired primary surveillance systems. The application of hybrid risk metrics to model and predict the development of risks and incidents also can enhance the reaction to an incident situation and enables the stakeholder to react more effectively and efficiently to limit the effect and damage of an already occurred incident. The guidelines and tools developed in HyRiM will support stakeholder to estimate the importance and priority of mitigation and recovery measures and provide therefore a sound basis for valid management decisions.

Pillar 4: International cooperation of stakeholders and policy makers

A main goal of HyRiM is to provide input to standardization and legislation activities on European level. This supports unification and enhances comparability of the results of risk assessments supporting the cooperation between stakeholders not only on national but also on European level as well as policy makers. In particular, the reliability and stability throughout the interconnected utility networks will be increased due to harmonized and enhanced risk management guidelines covering multi-dimensional security aspects of utility networks.

Pillar 5: Criteria for European Critical Infrastructures in the ICT sector with respect to SCADA

HyRiM provides input for finding criteria for standardisation activities on European critical infrastructures. In particular, new threats by the growing interconnection between utility networks and the usage of modern fixed and mobile communication infrastructures are investigated. Both SCADA systems and personally owned electronic communication devices are based on the same communication paradigm and standard (IP-networks). This leads – besides the high compatibility of diverse devices – to new threats and attack vectors, which are targeted by the hybrid risk metrics approach in HyRiM.

3.1.4. Societal Impact

Utility networks (e.g. power lines, water and gas pipes, etc.) and their respective providers are critical infrastructures that our society depends on, and permeates almost every aspect of our daily lives; thus the security research carried out in this project will have significant societal impact. Building on the checklist that is outlined in Annex 7 of the Guide for Applicants, we see HyRiM having societal impact in the following ways:

Ensuring security research meets the needs of society

There are a number of documents that highlight the societal security needs regarding protecting utility networks from cyber-attacks, and the need for safety and security in utility networks in general[84][85]. While system security in general and cryptography in particular, has come up with ingenious proposals to protect privacy and accomplish safety and security, trust is difficult to establish based on complicated technical security definitions commonly used in cryptography. The need for trust and reputation models has been recognized[86], but existing efforts towards the protection utility networks[87], do not follow a standardized approach. The degree to which utility networks are perceived as crucial for society is yet not in adequate relation to efforts regarding trust, risk and reputation models for utility networks. Achieving balance here is a major goal and impact of the project, whose necessity is also indicated by recent efforts of the German Informatics Society (GI), having set up a working group for the protection of critical infrastructures[88].

The cyber security threats that could lead to this significant societal impact could come from a number of different threat actors, including terrorists, criminal groups, insider attackers, and so-called hacktivists. Understanding and reducing the vulnerability of utility networks to these actors as well as estimating the potential risk coming from threat actors is a key outcome of the HyRiM project. As discussed earlier, the project will address these threats in a number of ways, including the development of methods and tools for risk assessment of interconnected utility networks, security architectures and guidelines for securing utility networks as well as their providers, and novel tools and processes that function in the context of these architectures.

Societal acceptance of these outcomes will be assessed directly in the context of WP5 of the project, building on the world-class experience and expertise of researchers at Energie Institut Linz. The research output of the project will meet the needs of stakeholders, and therefore society in general, through its programme of stakeholder engagement – and will be demonstrated as widely as possible in the contexts of WP5 of the project. There is a great deal of uncertainty about the potential impact of threats to utility networks, our research effort on risk assessment will endeavour to reduce this uncertainty.

Ensuring security research benefits society

The segments of society that will benefit from HyRiM research outcomes include the providers of utility networks, e.g. energy, gas and water providers, as well as their respective customers. Furthermore, associated standards and policy making organisations will reap the benefits of our research in terms of recommendations, guidelines, threat trends, and standards about necessary security and risk management guidelines applicable for utility providers of different areas. The general public will benefit from our research outcomes in a number of ways, in general through the development of more resilient and secure utility networks, which will ensure the availability of water

[84] European Network and Information Security Agency (enisa): *Protecting Industrial Control Systems Recommendations for Europe and Member States*, Deliverable -2011-12-09.
[85] European Network and Information Security Agency (enisa): *Smart Grid Security Recommendations*
[86] European Network and Information Security Agency (enisa): *Report on trust and reputation models Evaluation and guidelines*, 19 December 2011.
[87] IBM Intelligent Utility Network Solution, Sycamore Networks Utility Network Optimization, Actew Water Corporation:
http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/index.html,
http://www.sycamorenet.com/corporate/collateral/AN_utility_network_optimization.pdf,
http://www.actew.com.au/Customer%20Accounts%20and%20Services/Products%20and%20Services/Building%20and%20renovation/Preventing%20damage%20to%20utility%20networks.aspx
[88] German Informatics Society (GI), Working Group on Critical Information- and Communication Infrastructures (AK-KRITIS), http://fg-secmgt.gi.de/kritis.html.

and energy supply. More importantly, the quality of protection of the utility network will be presented not as a coarse grained statement that globally covers security as a whole, but via a set of indicators that relate to security and safety in different regards and aspects of the system. This will better establish trust though making security assurances more transparent and understandable for customers and society in general. As already pointed out above, utility networks are understood as critical infrastructures affecting society as a whole in times of failure or crisis. Using the measures and guidelines proposed by HyRiM, the probability of failure can be reduced and the resilience in times of crisis improved. Therefore, by ensuring secure and resilient future utility networks – the ambition of the HyRiM project – European societal values around maintaining the provision with basic supplies like water and energy, e.g. by minimising the downtime of a utility network, and sustainable development will be enhanced.

Ensuring security research does not have negative impacts on society
We take seriously the need to ensure against any negative societal impacts, with respect to rights and values, emerging from our research. As emphasized in WP4, protection of utility networks is to some extent a matter of surveillance. In this particular regard, we will carry out our research while assuring that the privacy of people is not violated by any surveillance technology proposed in the project (e.g., if personal communication devices of employees are temporarily activated as additional sensors). This research will strongly focus on risk assessment and measures, which per se do not release any confidential or sensitive information in general, besides attack strategies and threats to the system. However, the data upon which these measures are derived is collected in a way that is going to respect people's privacy and adhere to ethical guidelines. We will use the European Charter of Fundamental Rights as core guidance in ensuring against negative impacts on society from our research, including in critical areas such as inadvertent discrimination against specific societal groups.

3.1.5. Expected impact from individual HyRiM partners

In addition to the overall expected impact, HyRiM partners anticipate the following impact from the programme of work carried out by the project:

Partner	Expected impact
AIT	Cyber security risks are counted among the most important threats regarding utility networks and their providers. Measuring risk in this domain is very challenging, since the cascading effects of threats in interconnected networks are difficult to capture and no direct experience or tools to make assessments are available. The capability to understand risks is the basis for a critical infrastructure, such as a utility provider, to make informed decisions about required security measures. The methodologies and tools for risk assessment and management developed in the HyRiM project is envisioned to greatly increase the knowledge and transparency with respect to the organisation's understanding of risks associated with interconnected networks and how to monitor and implement controls to reduce them. As a result, the outcomes from HyRiM will have an impact on the technologies and organisational processes for risk assessment among the utility providers. High assurance is a core requirement in critical infrastructures just like utility networks and providers. The HyRiM security architectures and guidelines will equip utility providers with the necessary means to choose and build their systems to meet the high-assurance requirements. Further, with the methodologies and tools developed in the HyRiM project utility providers will be able to build secure and resilient networks structures. The best practices and vision of security issues as well as the methodologies for risk assessment developed as part of the HyRiM project will be usable by a broad spectrum of industrial bodies, policy makers and end-users. This ensures that the impact of HyRiM project results can be as wide as possible.

ULANC	Lancaster University's primary contributions are in the areas of 1) network security and quality of service, 2) the security of SCADA systems, 3) the ethnographic study of systems and human-system interaction and 4) the analysis of risk. The expected impact of Lancaster's contributions to HyRiM will mainly involve the application of this expertise, and its integration with the expertise of other project partners. In particular we expect to have an impact through: 1) taking past work on anomaly detection and broadening and generalizing this so as to produce a general, hybridised approach to assessing vulnerability and resilience in networked infrastructures operated by utility providers; 2) investigating how both vulnerabilities and resilience are created from the way that a utilities organisation interacts with its technological infrastructure; 3) developing reference architectures and frameworks that can be applied to analyse risk in a sociotechnical utility system. The expected impact will be on the practice of improving security in utility organisations, through the development and dissemination of the results, and also on the academic community through the publication of the work in scholarly journals in several subject areas, particularly those of human computer interaction, critical infrastructures and risk analysis.
UNI PASSAU	Utility networks are the backbone of our every-day life. This makes them a suitable and valuable attack target. The increasing threats from cyber-attacks make it necessary to not only to evaluate and quantify physical, but more than ever also existing and future cyber risks. Existing methodologies in this area are not sufficient, as newer technologies, such as, e.g., the Internet and other SCADA systems, form a system that can be described as a network of networks, which merges the currently isolated utility networks with a communication infrastructure. This lead to a completely new environment with potential unforeseeable consequences, especially in the fields of security and safety. Hybrid risk metrics promise to be a sufficient tool to derive new metrics that will be able to cover the new properties of these interconnected utility networks. The results of the HyRiM project can be used in future utility infrastructures to tackle both already existing threats, as well as newly arising ones, which originate from the formation of the previously described network of networks. Also, HyRiM will overcome several existing limitations of surveillance technologies, as inflexibility and missing self-security by evaluating the usage of novel, on-demand, ad-hoc systems that can be used to provide surveillance-capabilities in cases of failures in the primary system. Self-diagnostic measures will be assessed, which allow the monitoring of the perimeter and the internal states of the complete network to derive on-the-fly risk assessments which can be utilized to decrease the probability of high-impact failures. The combination of these solutions into practical guidelines and standards will have a strong impact on both national and European level, as it will enable utility providers to increase both the safety and efficiency of their infrastructure.
ETRA	The results of HyRiM will be applied to different areas and activities in order to protect the exiting utility networks and critical infrastructure making them more reliable and protect them through new threats trends. HyRiM will also provide a better overview and handling of security incidents than currently exists. All the results of the project will be focused to end-users (operators) of these critical infrastructures, giving them better understanding of their infrastructure and potential risk and threats in order to avoid or minimize their impact. However, the implementation of HyRiM results will also impact directly on the European citizens who depend on numerous Critical Infrastructure systems for services that are essential to their everyday lives, such, water supply, electricity, gas, transport, traffic, etc. By successfully defending Critical Infrastructures against attacks, potentially catastrophic events affecting society can be mitigated, protecting lives of European citizens. In this context, from an economic perspective, attacks on these network utilities

	and critical infrastructure is getting better and better organized internationally and widely implementing. In this context, the implementation of the results coming from HyRiM will avoid lots of losses caused by different types of attacks on these types of infrastructures.
AKH	If in one hand the development, the security and the quality of life in developed countries depends increasingly by the correct and continuous operation of a grid of interconnected utilities in the other the developed countries treated by terrorism actions. This is confirmed by recent attacks. On July of 2010 the Belarusian company VirusBlokAda discovered an especially designed worm for SCADA systems on a computer in Iran called Stuxnet . Stuxnet was specifically tailored to modify processes under control of Siemens' WinCC/PCS 7 SCADA software. Other well-known cyber-attacks against CIs have been reported before, like the one at Marrochy Water Services in Australia or the one at Davis-Besse nuclear power plant in Ohio. In the last case the SQL/Slammer worm broke in the nuclear power plant's security management system, leaving it unavailable during five hours. For the current situation is essential to understanding the problem and understanding what can be the impact of this problem in your system and in all the systems that are connected to yours. Only a Europe able to measure this new risk will be able to face it and apply all the necessary countermeasures.
ECA	The attacks to utility networks, for example to a SCADA system, may cause disastrous damages that will affect to a large extend the overall performance and stability of the critical infrastructure. Protecting and defending these utility networks against attacks and threats via different tools and methodologies is a challenging task, necessary in order to avoid great economic losses of the utilities operators, such as ECA, and to assure better services to the consumers.
LINZ	The gathered Know How and experience in implementing and using the approaches developed as part of the HyRiM project will be used to convince partners and regulation authorities that the HyRiM research outputs shall be considered for implementation in other entities as well.

Table 15: Expected impact from individual HyRiM partners

3.2. Dissemination and exploitation of project results, and management of intellectual property

3.2.1. Dissemination activities

Dissemination of project results is essential for HyRiM and it is the mission of the project that all results will be widely disseminated to relevant parties. Work Package 6 describes well-developed and efficient mechanisms for dissemination of project results which will be further detailed in a *Dissemination Master Plan*, and will ensure the successful dissemination to pre-identified target groups (e.g. end-users, standards and regulatory bodies, the general public, research community).

To enable the ambitious impact of HyRiM to be achieved, the general dissemination activities planned are described in Table 17. Therein, topics like the planned workshops, knowledge transfer, social media activities and press releases are covered in detail. Publication activities like attending relevant conferences and publishing articles in scientific journals are covered in Tables 18 to 21. These 4 tables include detailed information on conferences, which project members plan to attend, and journals, in which project members plan to publish the RTD results. Additionally, since guiding standardisation is an important topic of the HyRiM project, Table 22 lists a number of standardisation bodies, which are potential partners towards standardisation.

The Master Dissemination Plan will be presented in deliverable D6.1.

Dissemination Action	Description
Dissemination of project results in workshops	HyRiM will organise workshops to bring project partners, (extended) Advisory Board members, and external organisations and experts together to exchange ideas and disseminate project results, including the demonstration of attack scenarios. During the project preparations phase, a number of organisations have been contacted, and some of them explicitly expressed their interest in the project and thus were included in the Advisory Board. In the course of the project, additional organisations and experts will be continuously identified and contacted to be invited as external participants to HyRiM workshops.
Publication of deliverables	The HyRiM project will aim to make deliverables publicly available. All documentation will come with a Creative Commons License. The reports and tools resulting from the project will be distributed through the project's website. Before publication, the SSC will check the deliverables such that no sensitive information (personal data, classified information, etc.) is made public.
Publication of RTD results	Publishing of RTD results to the wider scientific communities through refereed journal publications, (chapters in) books, and conference proceedings (see below for a list of target outlets). The experience and reputation of the core technology partners guarantees the success of scientific dissemination of the results in the HyRiM project.
Transferring knowledge	This includes research exchange, the provision of workshops for professionals on the integration, maintenance, and deployment of the architecture, methodologies and tools for future users, and training for stakeholders.
Project liaisons	Establishing contacts and liaisons with existing initiatives, such as on-going research projects, and European and national initiatives is at the focus of the HyRiM project to increase the project's visibility in the community.
Networking	Building communities of actors and users through continuous networking activity. Due to members of the advisory board as well as the participants of the project workshops, the HyRiM project members are able to address a large community of international experts.
Public industry demos	Organising and animating industry outreach and end-user days. We will put a special focus on demonstration activities in different forms of the possibilities that the newly developed technologies will offer. The target audience will be relevant industry, institutional, public and research actors, whose main focus is the risk management and security of utility networks. The participation of globally acting partners will provide an additional, global dimension to our dissemination programme.
Social Media Activities	The overall motivation for the project as well as intermediate results and end-user application demos can be visualized in small video sequences, slideshows and animations, to be uploaded on Youtube or Slideshare, for example. This initiative has the potential to dramatically increase HyRiM's visibility even outside the scientific domain. Wherever appropriate the project will make use of other social media to disseminate results, such as Twitter.
Press releases	Publishing press releases about completed milestones. The HyRiM consortium will publish press releases about important milestones, public availability of new methodologies or software components. The consortium members will actively seek press interviews in online technological forum, newspaper, magazine, radio, TV etc. Distribution channels will be research and technology related news websites, press release channels, and mailing lists.

Table 16: Dissemination activities

HyRiM will mention the EU's subsidy in all promotional material, and will feed back into the EC by means of a set of success stories that will show the project's positive progress. Interaction with legislators, for example through reporting and consultations issued by the EC, will also be carried out, to make recommendations on the security legislation of utility networks and providers or inclusions for future legislation regarding the security of utility networks and providers. The work from HyRiM will be used to contribute to the on-going development of national and international security codes of practice and standards for utility networks, through liaison with EU and national authorities. The following further specific actions will be undertaken:

The HyRiM Website

The HyRiM website will be set up from the beginning of the project and maintained throughout the project with information, events and achievements. It will disseminate the HyRiM results and promote the project as one that addresses security of utility networks to a broad audience, especially within the research, industry and the end-user communities.

Participation in congresses, conferences, and workshops

Active discourse with peers at high quality academic and industry congresses, conference and workshops in areas related to the security of utility networks as well as providers and associated issues is essential to validate and strengthen the quality of the project's results. Furthermore, these outlets provide a rapid and direct dissemination avenue to research communities and end-users. To this end, the project will actively engage in participation in events in two broad areas: general security and communications outlets, and those related directly to utility networks and providers. A list of candidate outlets has been drawn up, many of which the project consortium already have previous experience of attending.

Venue
ACM Conference on Computer and Communications Security (CCS)
IEEE Symposium on Security and Privacy
IEEE International Conference on Computer Communications (INFOCOM)
IEEE International Conference on Communications (ICC)
IEEE Globecom
ISOC Network and Distributed System Security Symposium
International Symposium on Recent Advances in Intrusion Detection
IEEE Communications Society/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks
It-sa
D-A-CH Security
ISSE
BSI IT-Sicherheitskongress
CSIT World Cyber Security Technology Research Summit
Spanish Technological Platform for Security and Trust Technologies Esec
Spanish Technology Platform on Industrial Safety
ISMS Forum, the Spanish Association for the Promotion of Information Security
OMS Konferenz

Table 17: Candidate security and communication congresses, conferences and workshops

Venue
SCADA & Smart Grid Cyber Security Summit
Smart Grid World Summit
ACM/IEEE Conference on Information Processing in Sensor Networks (IPSN)
ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)
ACM International Conference on High Confidence Networked Systems (HiCoNS)
Hybrid Systems: Computation and Control (HSCC)
IEEE Conference on Decision and Control (CDC)
IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS)
American Control Conference (ACC)
ISCRAM, International Conference on Information Systems for Crisis Response and Management
IFAC Workshop on Distributed Estimation and Control in Networked Systems
The Annual Meeting of Security Control Centers and Network Control Systems
INTEROP – IT Expo and Conference
Network Automation
BlackHat
DEFCON
Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
Conference on Critical Information Infrastructures Security (CRITIS)
International Conference on Smart Grid and Clean Energy Technologies
Kommunikation in der Automation (KommA)
Large Installation System Administration Conference
Annual Computer Security Applications Conference (ACSAC)

Table 18: Candidate utility related congresses, conferences and workshops

Publication in Scientific Journals and Magazines

Similar to conferences and workshops, there are a number of related high-profile scientific journals the project will target. As commonly applied in large-scale projects, in the first two years predominantly conferences and workshops are targeted in order to discuss ideas with other experts in their related fields, and to spread first results of HyRiM. Finally, in the third year, we aim to publish journal papers to achieve higher impact in the community. Some potential targets are listed below.

Journal	Impact Factor
ACM Transactions on Information and System Security	0.600
IEEE Security & Privacy	1.172
IEEE Transactions on Communications	1.68
IEEE Transactions on Smart Grid	N/A
IEEE Networks	2.239
IEEE Globecom	N/A
Springer International Journal of Information Security	0.421
Information Security Journal: A global Perspective	N/A

The Cyber Security Journal	N/A
Leadership Journal	N/A

Table 19: Candidate target journals in the area of security and communications

Journal	Impact Factor
IEEE Transactions on Automatic Control	2.11
IEEE Transactions on Computer Systems	N/A
IEEE Control Systems Magazine	2.491
International Journal of Critical Infrastructures	N/A
Elsevier Automatica	2.829
Elsevier Computer Networks	1.200
Elsevier Future Generation Computer Systems	N/A
International Environmental Agreements: Politics, Law and Economics	1.659

Table 20: Candidate target journals in the area of critical infrastructures & utility providers

Participation in standardisation bodies

An important impact of the HyRiM will be toward guiding standardisation. The project will target the following standardisation bodies with outcomes from the project:

Standardisation Bodies
European Network and Information Security Agency (ENISA) http://www.enisa.europa.eu/
DIN, German Institute for Standardisation http://www.din.de
Bundesamt für Sicherheit in der Informationstechnik (BSI) https://www.bsi.bund.de
European Committee for Standardization (CEN) www.cen.eu
European Telecommunications Standards Institute (ETSI) www.etsi.org
IEEE http://www.ieee.org
American National Standards Institute (ANSI) http://www.ansi.org/
International Electrotechnical Commission (IEC) http://www.iec.ch/
Internet Engineering Task Force (IETF) http://www.ietf.org
Distributed Management Task Force (DMTF) http://dmtf.org/
International Society of Automation (ISA) www.isa.org
VDI/VDE http://www.vdi.eu/ http://www.vde.com

Table 21: Targeted standardisation bodies

Partner Specific Dissemination Plans

In addition to the overall project dissemination plans, partners have the following individual dissemination plans:

Partner	Dissemination Plan
AIT	As AIT is strategically positioned as a key player in the Austrian and European innovation system by performing applied research for and enabling the market exploitation of innovative infrastructure related R&D solutions, AIT has the advantage to disseminate HyRiM project results to industry and public organisations through a network which has been long established from collaborations on various cooperative and contract research projects.
ULANC	The dissemination plan for Lancaster University is to publish the work in 1) reports and seminars for the industry, in conjunction with the project partners; 2) conferences that extend across both the practitioner and academic communities (such as the Society for Risk Analysis annual conference); 3) scholarly journals in the relevant subject areas. These areas include risk studies (for which the most appropriate outlets would in this case be Risk Analysis and the Journal of Risk Research), critical infrastructure studies (International Journal of Critical Infrastructure Protection, International Journal of Critical Infrastructures), and human computer interaction (Mark Rouncefield is on the editorial board of Computer Supported Cooperative Work). Publications in the security and networks literature would be developed in conjunction with other project partners.
UNI PASSAU	The University of Passau is interested in disseminating results of this project within national and international networks. Especially, the University of Passau is partner of the following security-, safety- and utility-network-related networks: • Network of Excellence in InterNet Science (EINS; ICT, NoE, Call: FP7-ICT-2011-7, Project/Grant Number: 288021); • Energy efficiency in large scale distributed systems, funded by EU (COST Action IC0804); and • The Bavarian IT Security and Safety Cluster (registered member of the “go-cluster” initiative: http://www.go-cluster.de/de/innovationscluster/bayerisches-it-sicherheitscluster) Furthermore, the University of Passau will be attending or taking part in professional conferences and events. It is expected that outcomes of the project's research will appear in journals, such as listed in Table 20 and Table 21. Some of the most interesting conferences in which project outcomes could be published are noted in Table 18 and Table 19. The University of Passau will help to disseminate project results to industry and other research organisations in Europe. Close cooperation with other national and international projects are possible, e.g., the EU FP7 project EINS, ERDF project SECBIT, or EU FP7 project All4Green. Furthermore, the acquired knowledge and the results of the project will be used as contributions to international standardisation.
ETRA	ETRA will present HyRiM progress and results in the Spanish Technological Platform for Security and Trust Technologies Esec-, in the ISMS Forum, the Spanish Association for the Promotion of Information Security and in the Spanish Technology Platform on Industrial Safety. In addition, ETRA plans to disseminate the project results by means of publications in journals and magazines and also in different conferences and workshops. ETRA plans journal publications for the later phase of project when the results and findings of the project research will be available. As a first approach, ETRA has identified the scientific journals and magazines presented in Tables 18 and 19 to disseminate its research results and findings. Through the submission of papers and posters in the most relevant conferences, ETRA plans to show the project objectives and results.
AKH	Akhela will disseminate HyRiM results, adding to his web site an abstract of the project and its most relevant result, and a link to the project web site. Furthermore the

	project will be presented internally using the so called “cross-fertilization seminars”, where personnel not only of Akhela will be invited, and externally using the commercial network and its own more academic network (for example Akhela is a member of Serit -the Italian Platform for security- and an active member of the IMG-S - Integrated Mission Group for Security.)
ECA	Alginet plans to disseminate the project results with other electrical cooperatives, who will take profit of the new developments on security on smart grids. Actually, the electric cooperative of Alginet is member of ASEME (Association of Electric Companies), who in turn is member of GEODE (Groupement Européen des entreprises et organismes de Distribution d’Energie) organization and the electric cooperatives federation. Therefore the electric cooperative will take advantage of the general meetings with the different associations, in order to organize workshop and presentations of HYRIM project.
LINZ	LINZ will present experiences and project findings as well as shaping security awareness to increase the security and safety in utility network infrastructures. We will initiate talks and discussions with the regional and national utility providers and associated authorities, and inside professional associations covering the field of utility provision. LINZ is continuously working with these parties, so it will be easy to arrange appointments dedicated to the security and protection of utilities. The target will be to ensure a safe and secure operation of utility infrastructures in order to have a positive impact onto the reputation of the companies, to the benefit of their customers and even having an impact on national economics.

Table 22: Partner specific dissemination plans

3.2.2. Exploitation

Exploitation of the research results is an important part of HyRiM and an area of activity that requires a professional marketing approach, in order to achieve a successful transition from the research based level to the product/service based level. The project’s outcomes will comprise a wide range of technical as well as intellectual solutions. In particular, we foresee the following exploitable outcomes from the project:

- Open protocols, languages, schemas, etc.
- Patents on algorithms and other IPR
- Software tools

The project consortium members have the following plans to exploit the project’s results:

Partner	Exploitation Plan
AIT	AIT’s exploitation strategy for the HyRiM project is based on three pillars: leveraging of know-how, application of methodologies, and usage of developed toolsets. AIT contributes to the HyRiM project concentrate around the development of methodologies for risk assessment and security best practice guidelines for utility providers. This is a continuation of the efforts in other national and international research projects, directly in the area of utility providers and critical infrastructure protection, with the work on information security management and secure system design. The know-how gained from the HyRiM project will be leveraged in future research projects. Furthermore, the methodologies developed in the HyRiM project will give AIT the possibility to further extend its activities in applying and disseminating risk assessment and security best practices in contract research projects related to critical infrastructure in general, and specifically utility providers. While existing methodologies are used for this endeavour, HyRiM results will provide new and specific methodologies for utility providers, which is a specific focus of AIT. The tools developed in the HyRiM project, in addition to being applied in the pro-

	ject, are expected to be used in other contract research projects as the basis for developed tools. This will be done in line with AIT's strategic mission of transforming research results into industry applications in contract research or as a starting point for spin-offs.
ULANC	The main exploitation route for Lancaster University will be the identification and proposal of further projects that develop on the outcomes of this work. Concern with critical infrastructures, their increasingly networked and interdependent nature, the vulnerability of global supply chains that depend on them, all in a society that is increasingly preoccupied with risk, mean that this work will have a strategic significance in the years ahead. Models and tools that help integrate the treatment of technical and social vulnerabilities are also likely to become increasingly needed.
UNI PASSAU	The University of Passau will focus its contribution on the perimeter security and safety by surveillance technologies and will exploit the research results and experience gained in the HyRiM project in several dimensions: First, the results will directly improve the current lecturing activities of the University and the research knowledge gained during the project duration is expected to be incorporated into graduate, master's and doctoral programs. With an already strong profile in the area of IT-security and functional safety, the University will be able to further enhance and adapt the lectures to include not only classical network infrastructures' risk assessment and safety analysis, but also SCADA and utility networks. Second, by exploiting the activities in HyRiM, new input to research projects will be obtained. The results of the project will be used to further investigate the critical security and safety challenges in utility networks. The incentives and results derived from the project are expected to be used in the proposal writing of future projects and fostering further collaborations both with industrial and academic partners. Third, to strengthen the knowledge transfer between the academic and industrial world, both the research results and the tools developed in the project will be used to create further cooperation with the University's industry partners in the form of, e.g., contract research. Possible joint ventures or other forms of collaborative synergy-providing organisations will be investigated.
ETRA	ETRA's annual turnover and number of employees have increased uninterruptedly over the last 20 years to reach the current 250M€ and 2.200 staff –figures corresponding to 2010-. User-orientation combined with advanced technologies and innovative business models have been the drivers behind this sustained growth. ETRA's areas of activity are centered on Mobility, Energy, Public Services and Security. Over the last years Security has evolved into a Business Area (BA) which not only has developed vertically but also horizontally, cutting across the rest of the BA,s. ETRA's customers are typically public authorities and large companies who use our large scale real-time control systems and information management services to run mission-critical and sometimes life-critical operations in the area of Smart Grids. The protection of CI is at the core of the technical and business interests of ETRA, with a currently associated annual turnover of approximately 120M€, expected to grow by a 10% per year over the next 5 years. HyRiM is expected to have a direct impact on this huge business area, complementing the rest of research and development initiatives where ETRA is taking place.
AKH	The LE partner Akhela will use HyRiM results to upgrade its offer in the security sector. Akhela has been present in the security market for critical infrastructure (mainly Oil & Gas Market) since the begging. Recognising that the security management is a strategic factor for organisation, Akhela offers not just security products and services, but prevalently know-how, solutions, processes and answers capable of effectively meeting the security needs of an organisation. Each solution is specifically targeted and continually updated to respond to the new

	security threats that emerge each day. Continual scouting of the international market enables Akhela to offer clients the most technologically advanced and reliable products and services. Akhela boasts an especially innovative range of offerings in the fields of application security and industrial security (SCADA/DCS networks). The results of HyRiM and the know out acquired will be used by Akhela to consolidate its own market and to exploit the possibility to enter in new business domains like water pipes, gas utilities.
ECA	The electrical cooperative of Alginet, being a non-profit organization, will concentrate its exploitation efforts in offering a better service to its clients and reducing economic losses, protecting their infrastructure from cyber risks and threats. CEA, as network operator will understand better their infrastructure and the potential risks, allowing the implementation of new policies and more secure infrastructure. Their exploitation plan is directly based on the use of HyRiM results in the SCADA system installed to increase the security of the existing infrastructure by adding the new tools and methodologies.
LINZ	Linz AG will include the project findings into the internal risk management of the companies utility control networks and surveillance systems. Appropriate measures can then be derived to strengthen these infrastructures.

Table 23: Partner specific exploitation plans

3.2.3. IPR Management

All partners have a joint non-exclusive right to exploit commercially all intellectual property produced by any participant in the project as a part of its work. The contractors should be granted a cost-free licence to use other partners' pre-existing intellectual property for the purposes of the project while the project is running; thereafter they should not be unreasonably denied a licence to use the property, although a commercial rate may be negotiated. This approach to knowledge management and IPR will be detailed and regulated in the Consortium Agreement, which will set the basis for a specific Exploitation Agreement. Some of the major aspects covered are indicated below briefly.

Confidentiality: Each partner will treat information from other partners as confidential and not disclose it to third parties unless it is obvious that the information is already publicly available.

Ownership of Knowledge: Knowledge is owned by the partners who carried out the work generating the knowledge, or on whose behalf such work was carried out. If a partner wishes to assign any knowledge to a third party he should inform the other partners and request their consent, which should not unreasonably be withheld.

Patents: Partners who own patentable knowledge may (and are encouraged to) at their own expense make applications for patent or similar form of protection and will supply details of each such application to the other partners.

Access Rights: Partners grant to each of the other partners royalty-free access right to knowledge generated in the project to the extent needed to successfully perform the project. Access rights to knowledge generated in the project and to pre-existing knowledge for use outside the project are, when needed to make use of the project result, given between partners in different WPs on preferential conditions. Access rights to knowledge generated in a WP, when needed to make use of the project result, is given royalty free to the other partners participating in the same WP. Access rights to a partner of pre-existing knowledge for use outside the project is, when needed and only to the extent necessary to make use of the project result, given on preferential conditions to the others partners in the same WP.

In addition to the Consortium Agreement that will regulate the IPR management, a specific exploitation plan will be set up during the first 12 months of the project and be reviewed yearly. It will be based on the preliminary exploitable results identified in Section 3. The consortium will pay specific

attention to IPR (management, early detection, protection). The partners will reach a full agreement, complementing the EC contract, on pre-existing intellectual property rights excluded from HyRiM and user licences in the consortium agreement. The basic rule is that each partner remains the owner of its background knowledge. The agreement will detail rights to exploit project results for commercial purposes; each partner will, however, maintain the right to use the project outcome for internal use.

During the life of HyRiM, the implementation of these IPR principles will comprise the following main tasks:

Updating of foreground knowledge: collect, update and maintain the list of major fore-ground knowledge (known as “pre-existing know how”) required to implement HyRiM. This includes the list of foreground excluded from HyRiM before the contract signature, as set up in the Consortium Agreement, and of other foreground identified throughout the project life.

Management of the HyRiM knowledge portfolio: collect information on the knowledge gained and agree with the owners of the knowledge the stand access conditions within the project. The HyRiM knowledge portfolio will also be the key tool for dissemination and exploitation of project results.

Knowledge projection: propose a general policy regarding co-ownership of knowledge and moderate solutions in case of co-ownership between different beneficiaries and provide advice about knowledge project when required (patents, copyrights, etc.).

Consortium Agreement maintenance and evolution: Maintain the Consortium Agreement and prepare corresponding decisions to be taken by the Steering Committee related to modifications of the pre-existing know-how, termination of participation and entrance of partners.

The implementation of these IPR principles and exploitation preparation will be under the responsibility of the Co-ordinator, who will report on a regular basis and whenever requested to the Steering Committee. In case of major conflicts that cannot be solved by the Co-ordinator, the Steering Committee will be called for resolution.

4. Ethics Issues[89]

ETHICS ISSUES TABLE

	Research on Human Embryo/ Foetus	YES	Page
	Does the proposed research involve human Embryos?		
	Does the proposed research involve human Foetal Tissues/ Cells?		
	Does the proposed research involve human Embryonic Stem Cells (hESCs)?		
	Does the proposed research on human Embryonic Stem Cells involve cells in culture?		
	Does the proposed research on Human Embryonic Stem Cells involve the derivation of cells from Embryos?		
	I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	YES	

	Research on Humans	YES	Page
	Does the proposed research involve children?		
	Does the proposed research involve patients?		
	Does the proposed research involve persons not able to give consent?		
	Does the proposed research involve adult healthy volunteers?		
	Does the proposed research involve Human genetic material?		
	Does the proposed research involve Human biological samples?		
	Does the proposed research involve Human data collection?		
	I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	YES	

	Privacy	YES	Page
	Does the proposed research involve processing of genetic information or personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?		
	Does the proposed research involve tracking the location or observation of people?		
	I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	YES	

	Research on Animals[90]	YES	Page
	Does the proposed research involve research on animals?		
	Are those animals transgenic small laboratory animals?		
	Are those animals transgenic farm animals?		
	Are those animals non-human primates?		

[89] See Annex 6

[90] The type of animals involved in the research that fall under the scope of the Commission's Ethical Scrutiny procedures are defined in the Council Directive 86/609/EEC of 24 November 1986 on the approximation of laws, regulations and administrative provisions of the Member States regarding the protection of animals used for experimental and other scientific purposes Official Journal L 358, 18/12/1986 p. 0001 - 0028

	Are those animals cloned farm animals?		
	I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	YES	

	Research Involving non-EU Countries (ICPC Countries[91])	**YES**	**Page**
	Is any material used in the research (e.g. personal data, animal and/or human tissue samples, genetic material, live animals, etc) : a) Collected and processed in any of the ICPC countries?		
	b) Exported to any other country (including ICPC and EU Member States)?		
	I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	YES	

	Dual Use[92]	**YES**	**Page**
	Research having direct military use		
	Research having the potential for terrorist abuse		
	I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	YES	

[91] In accordance with Article 12(1) of the Rules for Participation in FP7, 'International Cooperation Partner Country (ICPC) means a third country which the Commission classifies as a low-income (L), lower-middle-income (LM) or upper-middle-income (UM) country. Countries associated to the Seventh EC Framework Programme do not qualify as ICP Countries and therefore do not appear in this list.

[92] Dual-use items mean items, including software and technology, which can be used for both civil and military purposes (Ref: Article 3**,** Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items

5. Consideration of gender aspects

There are no gender-specific tasks or work packages in the content or work plan of HyRiM. Furthermore, the following measures are planned to encourage the involvement of women in HyRiM:

- All partners will be asked to engage or even to employ more women. Research institutions in particular are encouraged to motivate female students and scientists. When hiring new staff, women should be preferred where they have comparable qualifications. Actually for example the business unit of AIT involved in HyRiM has employed 5 women in scientific positions, one of which will be working in the project.
- HyRiM will further encourage project partners to facilitate a better balance between work and private life, by supporting flexible work time arrangements and distance working for project members, especially those with families with small children, to make it more viable for both parents to continue working.
- HyRiM will further present the project at university recruitment activities to encourage women to pursue a technical career within the field of computer security.
- Open House or lab visits for schoolgirls or female students will be organised, especially where demonstration systems or lab equipment that demonstrates HyRiM related technology can be shown.
- In the long run, all the above activities aim at improve the gender balance within the field of security research.

6. Security sensitivity Issues

It is NOT expected that the outcome of HyRiM will in itself be sensitive to the extent of being classified as “EU Secret”, “EU Restricted” or “EU Confidential”.

However, it is possible that sensitive information may be disclosed, either by project members or the Advisory Board, during the course of the project. The that end, the involvement parties will have the responsibility of not distribution such information in the project deliverables, and to ensure that classified material is archived in a safe and secure way until the classification expires. Material that is not vital for verifying project results may be returned to the information owners of may be destroyed using appropriate means. Classified information must only be distributed on a need-to-know basis to project member with sufficient security clearance.

Furthermore as a general rule with respect to the project deliverables, the policy will be maximising their diffusion to increase the project impact, but only to parties duly entitles to get them, that is:

- Members of the (extended) Advisory Board
- EC or EU member states authorities (national, regional or local)
- Companies or institutions operating or developing ICT systems for critical infrastructure

Last, but not least, it is noteworthy to mention that all industrial partners and most academic researchers in the consortium are used to handle security sensitive information and have the proper protocols and security clearances in place.

Annex A - Legal and Ethical Issues - User Consent, Privacy, Data Protection

This Annex defines how research experiments will be executed in the HyRiM project in order to respect local, national and EU ethical directives. In the following we describe:

1. How data is collected and protected;
2. The procedures and instruments the partners agreed on to ensure privacy; and
3. Compliance with the EU Data Protection Directive (Directive 95/46/EC)

The focal points issued in this context are

1. Copies of ethical approvals by the competent legal local/national Ethics Boards/Bodies/administrations must be submitted to the European Commission prior to the commencement of the research.
2. When submitting the application for scrutiny to the competent Ethics Boards/Bodies for authorization detailed information must be provided on the procedures that will be used for the recruitment of participants (e.g. number of participants, inclusion/exclusion criteria, direct/indirect incentives for participation, the risks and benefits for the participants etc.) and the nature of the material that will be collected (e.g. sensitive or personal data etc.)
3. When submitting the application for scrutiny to the competent local/national Ethics Boards/Bodies for authorization, detailed information must be provided on the informed consent procedures that will be implemented. Copies of examples of Informed Consent Forms and Information Sheets must be included. These must be in language and terms understandable to the participants. Participants must have the right:
   - To know that participation is voluntary
   - To ask questions and receive understandable answers before making a decision
   - To know the degree of risk and burden involved in participation
   - To know who will benefit from participation
   - To know the procedures that will be implemented in the case of incidental findings. The applicants must ensure, and document, the fact that a procedure is in place to take care of potential
   - incidental findings during the research is in place
   - To receive assurances that appropriate insurance cover is in place
   - To know how their data will be collected, protected during the project and either destroyed or reused at the end of the research. If it is planned to reuse the data, the participants must be duly
   - informed and consent also obtained for any further usage
   - To withdraw themselves and their data from the project at any time
   - To know of any potential commercial exploitation of the research.
4. When submitting the application for scrutiny to the competent local/national Ethics Boards/Bodies for authorization, the applicants must provide detailed information on privacy/confidentiality and the procedures that will be implemented for data collection, storage, access, sharing policies especially when third party countries are concerned, protection, retention and destruction. Confirmation that they comply with national and EU legislation must also be included.
5. In compliance with Directive 95/46/EC and 1/2010 Opinion of the Article 29 Working Group, a data controller dedicated to the project must be appointed.
6. Applicants must obtain instructions from their institution's data controller as described in Opinion 1/2010 Opinion. The technical data protection procedures that will be implemented in the project must be detailed. These instructions must demonstrate compliance of the data protection processes with the European legal framework. Copies of these instructions must be forwarded to the European Commission prior to the commencement of the related studies. If instructed by the data controller of their institution, applicants must consider obtaining approvals/opinions/notifications from their national data protection authorities for the proposed data collection and processing. If requested, copies of these documents must also be provided to the European Commission.

7. During the lifetime of this project the revised Directive 95/46/EC on Data Protection and Privacy may come into force, and the applicants may need to take this into account to ensure continuing compliance.
8. The applicants must provide a detailed description of the security measures that will be implemented to prevent improper data disclosure. The potential malevolent use of the project findings must also be examined by the applicants in consultation with the Ethics Advisory Board and Reported to the European Commission.
9. An Ethics Advisory Board must be established which includes employees' representatives together with one or more external, independent members with relevant experience in ethics to monitor the ethical concerns in this project. The work of the Ethics Advisory Board must be fully integrated into the management structure of HYRIM. A report by the Ethics Advisory Board must be submitted to the Commission with the Periodic Reports. In case the Board considers it necessary, the Chairman of the Board shall contact and inform the EC/REA.
10. Given the vagueness of the concept of ethnicity, and the risks it brings of discrimination and stigmatization, it is important to state clearly the hypotheses linking the ethnicity of workers to security. This information must be forwarded to the Ethics Advisory Board for its consideration and approval.

A1. Collection and Protection of Data

All sites will provide information on privacy/confidentiality, the procedures for participant recruitment and selection, data collection, storage, and destruction and how these comply with national and EU legislation, in particular FP7 Ethical Guidelines and the EU Data Protection Directive (Directive 95/46/EC).

How to treat the collected data:

i. The collected data will remain the property of HyRiM.
ii. The collected data will be kept securely at all times.
iii. The collected data will be kept on secure servers under the control of the research team at each experimentation site.
iv. The raw data will not be shared but the results of the experimentations will be shared to facilitate cooperative research amongst the partners.
v. Unless specifically requested and agreed, the collected data will be destroyed within 12 months of the completion of the project to allow for end of project dissemination and follow-up.
vi. Collection, storage, forwarding and destruction of data will be documented.

Risks of disclosure of identifiable information:

i. We will not identify subjects in our reports. Any inadvertent disclosure of private identifiable information will be avoided. If any information we collect is accidentally identifiable it will be neither sensitive nor potentially damaging.
ii. All data will be anonymised and in any report participants will be given pseudonyms. A list of participant identities and pseudonyms will be kept on a separate secure server solely in order to ensure that if participants choose to withdraw from the study, their data can be located and destroyed if required.
iii. Neither direct identifiers, such as names or email addresses, nor information that would allow someone to deduce our participants' identities will be used in reports about the experiments.
iv. If the information we collect might be identifiable in a situation, in which we cannot offer confidentiality, such as group discussions, every effort will be made to protect participant's identity in any kind of publication.

In D7.6 all partners will provide:

- Approvals for the intended data collection and processing.
- A detailed description of security measures that will be implemented to prevent improper use, improper data disclosure scenarios and 'mission/function creep'. In addition, the potential "unforeseen usage" implications of the experimentation will be examined and reported.

A2. Privacy Issues

A2.1. Ethical Consent Protocol

Each experimentation site will develop an approved ethical consent protocol within six months of the start of the project that will be submitted to the external independent Ethics Adviser and the Commission.

In more detail this means:

i. Ethical standards and guidelines compatible with, and equivalent to, those of FP7 will be rigorously applied, regardless of the country in which the research is carried out.
ii. All participants receive introductory descriptions about the HyRiM project and the purpose of studies applied at the experimentation sites.
iii. The Informed Consent Forms and all Information Sheets will be in language and terms understandable to the participants.
iv. All experiments are introduced as research and the purpose and procedure of the research will be introduced in an understandable way.
v. It will be emphasized that it is the potential participants' choice about whether to participate in the study.
vi. All participants will be informed of their right to privacy and the extent to which participation in this research may impact on their lives – for example by giving details of their family life – and the mechanisms the researchers have put in place to protect participant's privacy through processes of anonymisation and data storage and security.
vii. Participants will be informed about duration and effort to participate in any experiment.
viii. In any survey, people will be informed what kinds of questions we plan to ask, and we will make it clear that people can choose not to answer questions.
ix. Participants will be made aware of their 'withdrawal rights': they can withdraw from the research at any time and, if they wish, any personal data, recordings or images can be destroyed.
x. Contact information to the project´s stakeholders will be provided.
xi. Risks and benefits will be explained (»We do not anticipate any risks to study participants and there will be no financial benefits for people participating in this study«).
xii. If applicable, arrangements for insurance coverage for participation will be described.
xiii. Participants will be made aware of the complaints procedure, both to any local ethics advisor and to ELAB.
xiv. Participants will be made aware that they can ask questions and receive understandable answers before making a decision (e.g. giving consent, withdraw).

In D7.6 all partners will provide to the commission:

- Detailed information on privacy/confidentiality and the procedures that will be implemented for data collection, storage, protection, sharing policies, retention and destruction as well as confirmation that these procedures comply with national and EU legislation.
- Detailed information on the procedures that will be used for the recruitment of participants (e.g. number of participants, inclusion/exclusion criteria, direct/indirect incentives for participation, the risks and benefits for the participants, etc.) as well as the nature of the material that will be collected.
- The ethical consent protocols developed for each experimentation site.
- Copies of examples of Informed Consent Forms and Information Sheets.
- Copies of ethical approvals/opinions/notifications by the competent legal local/national Ethics Boards/Bodies/administrations.
- Copies of ethical codes and practices the research is subject to and compliant.
- Copies of instructions of the institution's personal data protection officials.
- Copies of the instructions of the respective data controller, if data is processed on the behalf of a partner (or the project represented by the project's data controller).
- Copies of instructions of approvals/opinions/notifications from their national data protection authorities, if requested.

A2.2. Releases for Images and Recordings

We will ask participants for permission to make any images or recordings that we will own and use in public ways – in workshops, conferences, presentations and journal or book articles. We will explain to the participants that we will ask them to indicate how we may use the images and recordings, after their participation in the study. Hence we will establish a mechanism that allows us to own and use a person's image or voice in specified, public ways. This will consists of a consent form that subjects sign giving the partners permission to use their voices and/or images.

The release will consist of:

i. The researcher(s) name and affiliation;
ii. A title for the research that is sufficiently descriptive to identify the study;
iii. A description of the material to be released;
iv. A list of ways how the material is used and how it will be securely stored;
v. A statement that signing the release is voluntary;
vi. The subject's agreement: written, recorded, or oral, depending upon the circumstances;
vii. Parental permission as well as child consent, if the subjects are minors; and
viii. Outline of complaints procedure to the ELAB.

To every subject, the option and process for destruction of the data will be explained. They may decide that, although they gave us permission to photograph or tape them, they don't want us to use their images or tapes after all. In this case, the photograph or tape will be destroyed with all data within 12 month after the project's end (according to Section A2).

A3. Compliance with the EU Data Protection Directive

During the lifetime of this project, the revised Directive 95/46/EC on Data Protection and Privacy will come into effect. The HyRiM project and specifically the ELAB will take this into account to ensure continuing compliance. This will be treated in Task 7.3 and will form an important aspect of the work of the ELAB. EU Data Protection Directive (Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data.

EU Directive 94/46/EC requires that:

- Notice: subjects, whose data is being collected, should be given notice of such collection.
- Purpose: data collected should be used only for stated purpose(s) and for no other purposes.
- Consent: personal data should not be disclosed or shared with third parties without consent from its subject(s).
- Security: once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- Disclosure: subjects, whose personal data is being collected, should be informed as to the party or parties collecting such data.
- Access: subjects should be granted access to their personal data and allowed to correct any inaccuracies.
- Accountability: subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

In the context of the Directive 95/46/EC, personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Article 2a). Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link. Examples of such data include address, bank statements, credit card numbers, and so forth. Processing is also broadly defined and involves any manual or automatic operation on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction (paraphrased from Article 2b).