Risk Management based on Bayesian Networks in Industry 4.0

Presenter: Mahsa Teimourikia, PhD

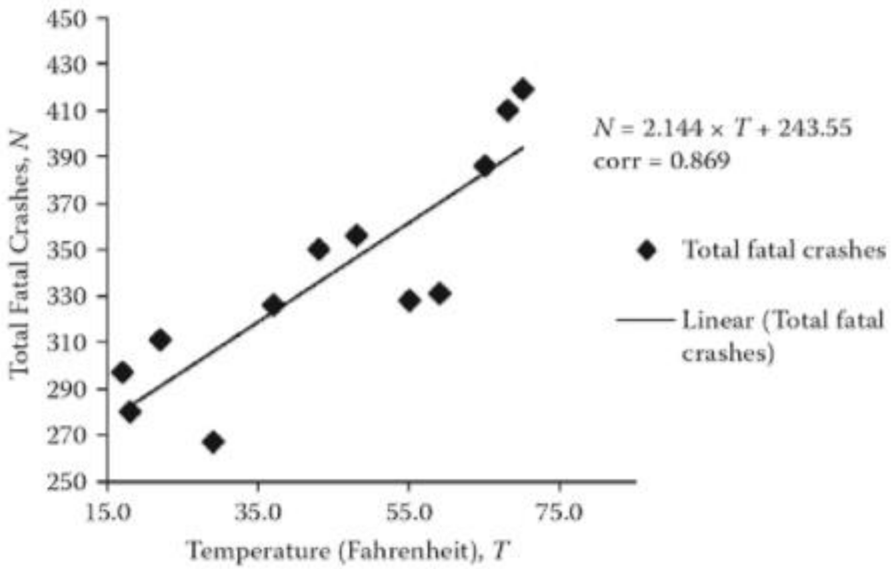
@R-Ladies

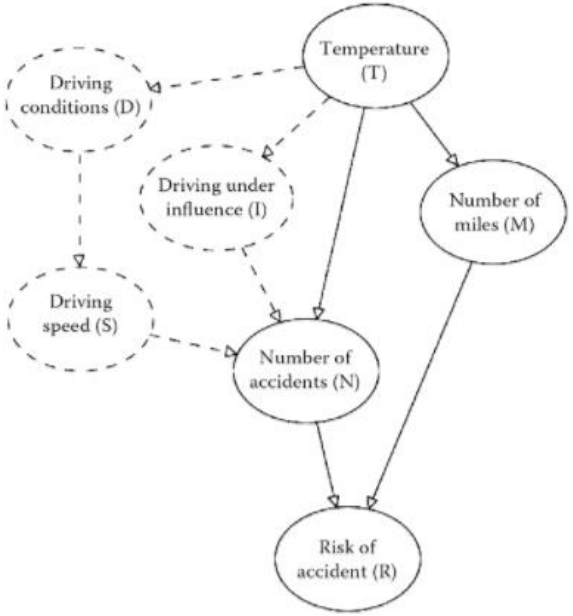
What is Risk Management?

- **Risk management** is the identification, evaluation, and prioritization of **risks.**
- **Risk management** is defined in ISO 31000 as the effect of uncertainty on objectives.
- The goal of **risk management** is to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.
- **Risk management's** objective is to assure uncertainty does not deflect the endeavor from the business goals.

The need for Causal, Explanatory Models in Risk Assessment

- For **risk assessment** the regression model is useless, because it provides no explanatory power at all.
- The regression model vs. a causal model to predict the number of fatal crashes based on the US Department of Transport data (2008):





The Limitation of Common Approaches to Risk Assessment

- The fact that some factors might be missing from the data does not mean that they should be ignored in the eventual risk assessment.
- There is a need to understand the cause and effect, and consider Subjective factors in addition to the available objective factors from the data.
- However, we should be careful about the person's ideology and the view of the world in the subjective analysis of causation.

Measuring Uncertainty: The Inevitability of Subjectivity

- Probability is the term used to quantify uncertainty about some unknown entity, which can be:
  - Events that we have good understanding of their uncertainty
    - The next toss of the coin will be a head.
  - Events that we have a poor understanding of their uncertainty
    - Italy will win the next World Cup
  - An “unknown” event
    - The bank will be forced out of business in the next two years as a result of a threat that we do not yet know about.
- Uncertain events are not just those that lie in the future. Because of incomplete information there is uncertainty about events such as:
  - O.J. Simpson murdered his ex-wife

Frequentist vs. Subjective Views about Measuring Uncertainty

- Frequentist definition of a chance of an event: If an experiment has n equally likely events, then the chance of any event in m/n. where m is the number of elementary events in the event.
  - Assumption 1: The experiment is repeatable many times under identical conditions.
  - Assumption 2: The outcome of one experiment does not affect the result of any subsequent experiment.
- In some cases, the two assumptions do not stand, e.g. there is a 1 in 10 million chance that a meteor will destroy the life on earth.
  - Here, we can only the **subjective measure of uncertainty** based on our **current state of knowledge**.

Bayes’ Theorem and Conditional Probability

- All probabilities are conditional!
  - P(A|K), where K is the background knowledge or context.
  - In practice if the same context K is assumed throughout an analysis, then it makes sense to simply write P(A) instead of P(A|K).
- The probabilistic reasoning involved in calculating P(A|K) include:
  - Starting from a hypothesis H for which we have a belief about P(H) called our **prior belief** about H.
  - Using evidence, E, about H to revise our belief about H in the light of E; in other words, to calculate P(H|E) called the **posterior belief** about H.
  - We know that P(H|E) = P(H) x P(H ∩ E), however we often don’t know the P(H ∩ E). Instead we often know the P(E|H) which is the **likelihood of the evidence E** given the hypothesis.

Bayes' Theorem and Conditional Probability

- Bayes' theorem gives us a simple method to calculate P(H|E) in terms of P(E|H) instead of the P(H,E):

$$P(H|E) = \frac{P(E|H) \times P(H)}{P(E)}$$

- Example: H: Patient has lung cancer; E: Patient is a smoker;
  - 5% patients in a clinic are diagnosed with lung cancer (Prior belief in H, P(H) = 0.05)
  - 50% of patients are smokers (Prior belief in E, P(E) = 0.5)
  - 80% of diagnosed patients are smokers (Likelihood of a cancer patient be a smoker, P(E|H) = 0.8)
  - What is a likelihood a new smoker patient be diagnosed with cancer? (P(H|E))

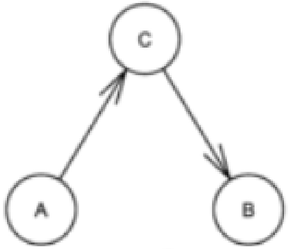
$$P(H|E) = \frac{0.8 \ \times 0.05}{0.5} = 0.08$$

What are Bayesian Networks?

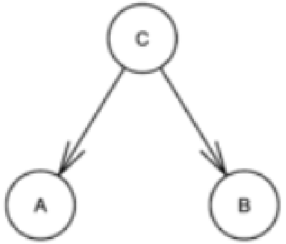
- We have seen how Bayes' theorem enables us to correctly update a prior probability for some unknown events when we see evidence about the event.
- In any real-world risk assessment problem there will be many unknown events and many different pieces of evidence, some of which may be related.
- When we represent such problems graphically, with all uncertain variables being represented as nodes and an edge between two nodes representing a relationship, we have a **Bayesian Network (BN).**
- A **Bayesian Network (BN)** is an explicit description of the direct dependencies between a set of variables. This description is in the form of a directed graph and a set of node probability tables (NPTs)

Structural Properties of BNs

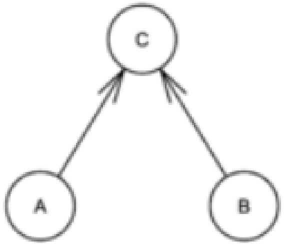
- In BNs the process of determining what evidence will update which node is determined by the conditional dependency structure:
  - Serial Connection: Causal and Evidential Trials
    - Any evidence entered in A will be propagated through C to B
    - Here A and B are conditionally independent given C



  - Diverging Connection: Common Cause
    - Any evidence entered in C will be transmitted to both A and B
    - Evidence at A is transmitted to B through C
    - Here A and B are conditionally independent given C

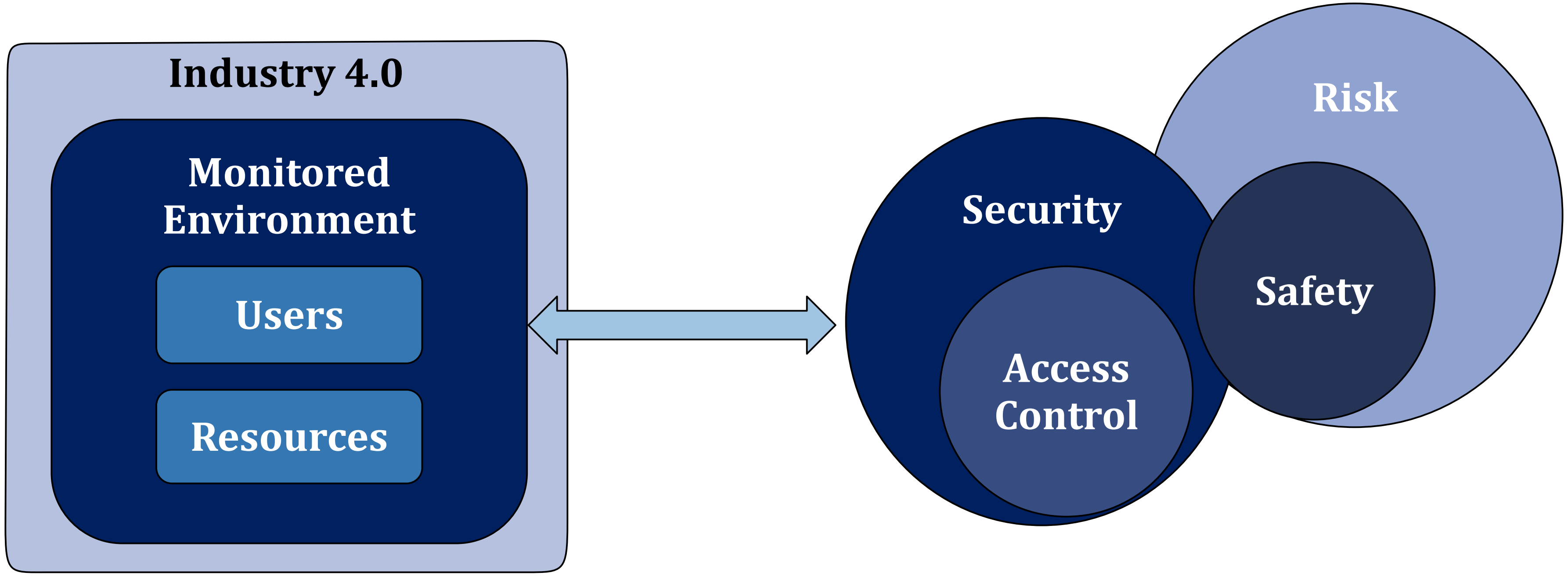


  - Converging Connection: Common Effect
    - Evidence at A or B will be transmitted to C
    - Any Evidence at C will be transmitted to both A and B
    - Here B is dependent on A given evidence at C



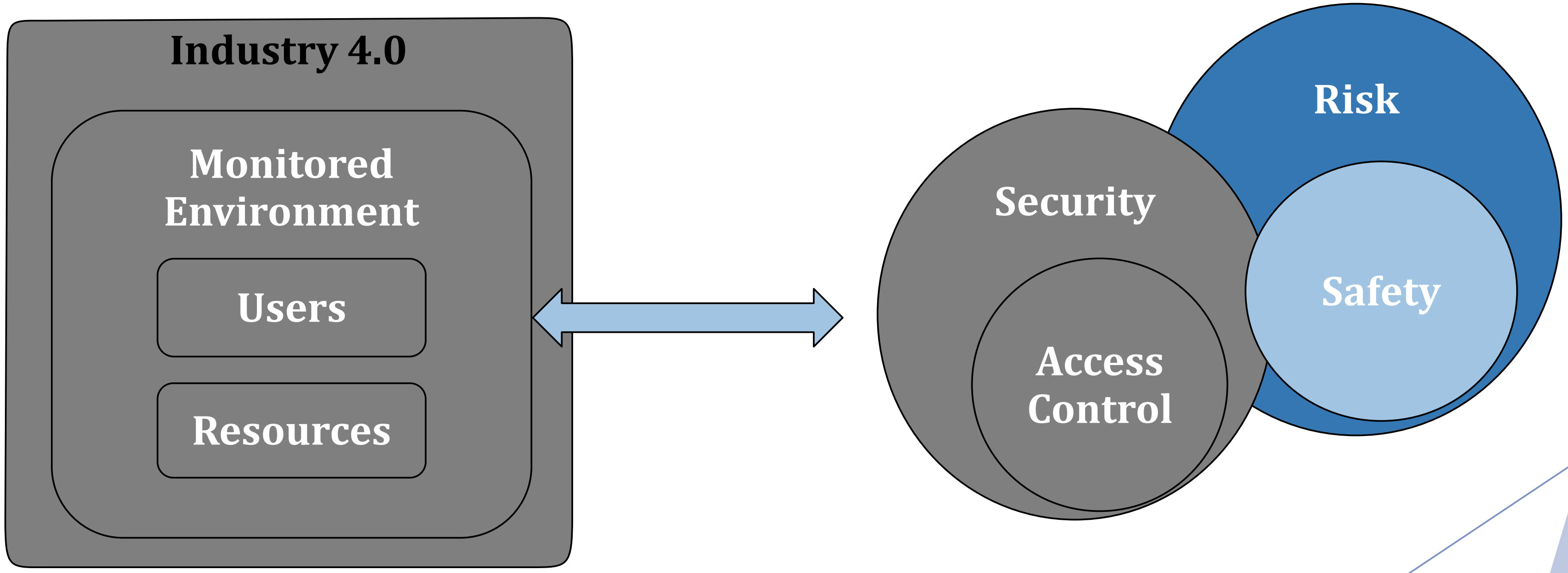
A USE-CASE: Co-Engineering Security and Safety in Industry 4.0

Defining the Main Concepts



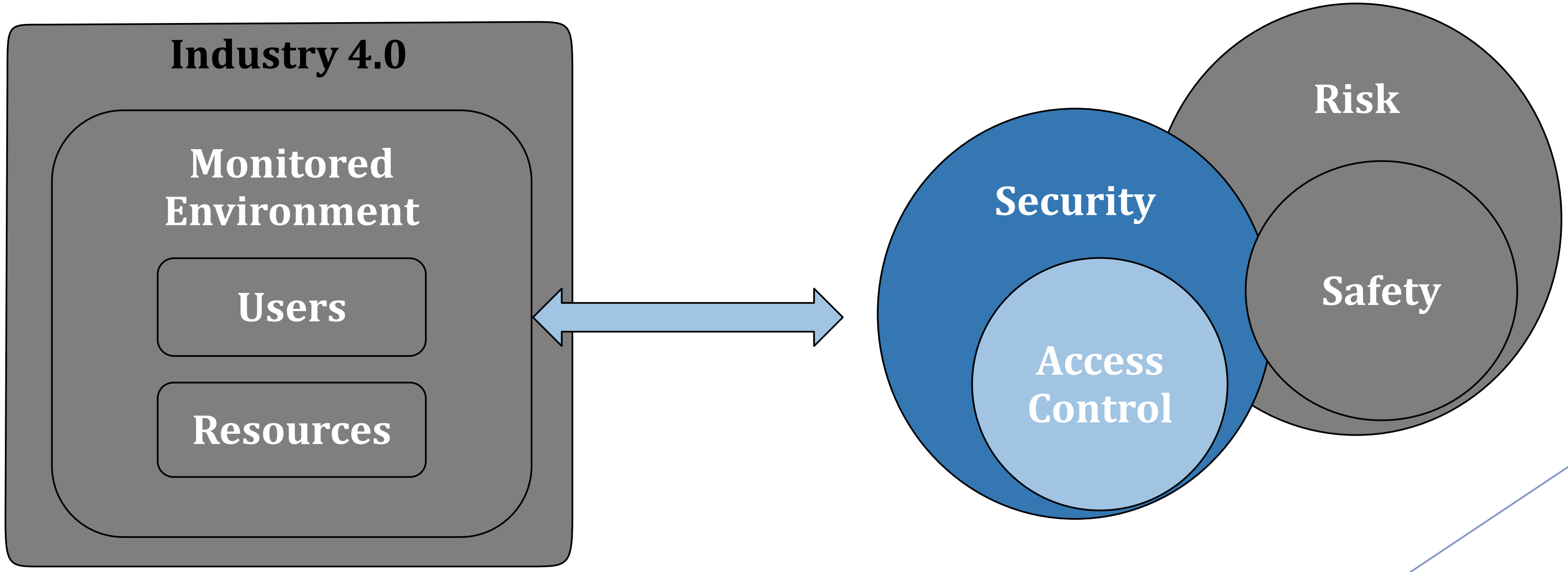
Defining the Main Concepts

- According to **ISO 31000**, **risk** is the “effect of uncertainty on objectives” and an effect is a positive or negative deviation from what is expected.
- Safety can be considered as a subset of risk that may cause harm to the health and life of persons, or cause harm or destruction of resources, and infrastructures in the environment.



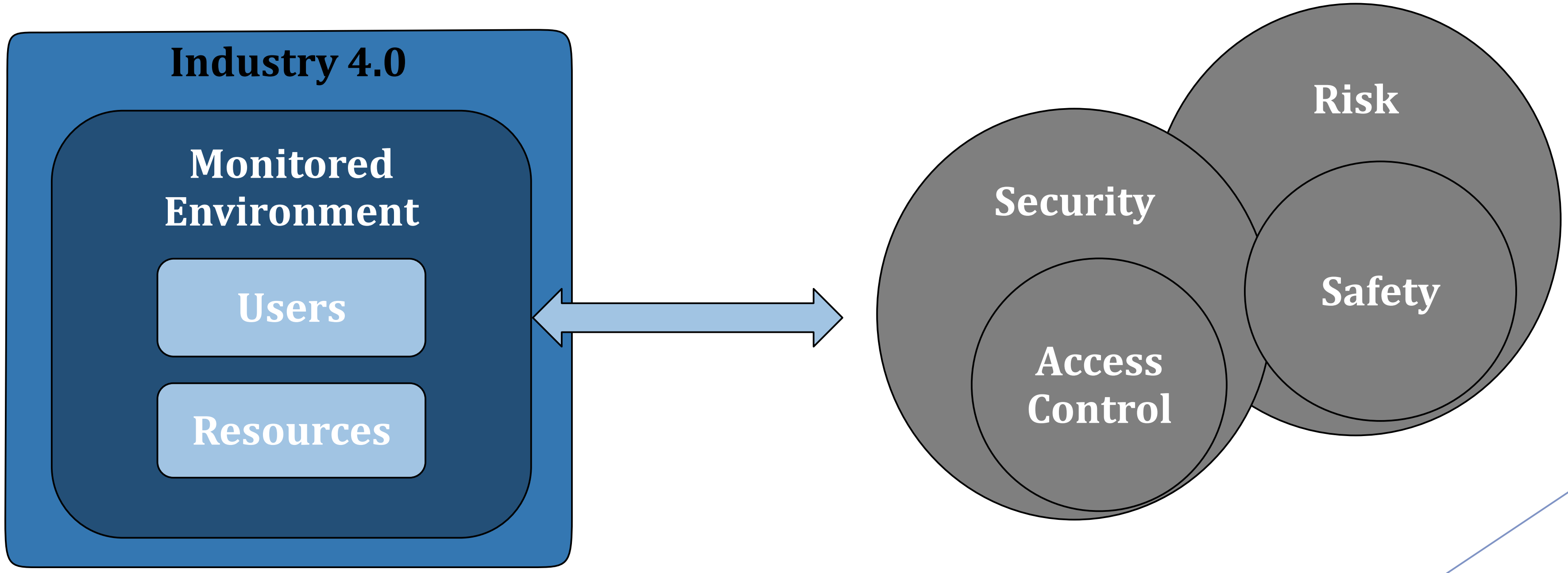
Defining the Main Concepts

- **Security** refers to the processes and methodologies which are designed to protect confidential, private and sensitive **assets** from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.
- More specifically, Access Control has the goal of limiting the actions or operations that a legitimate user can perform on the protected assets.

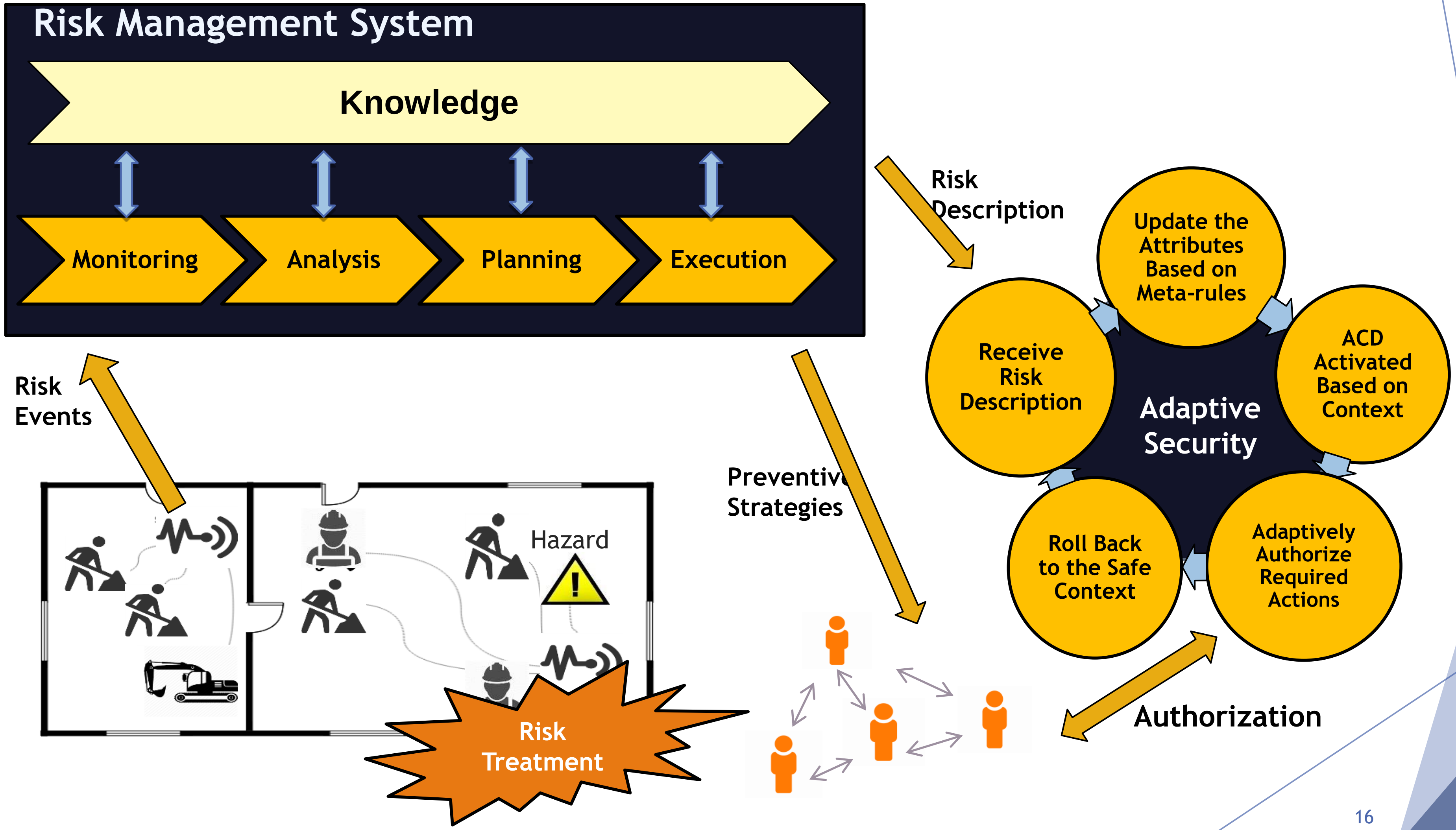


Defining the Main Concepts

- Industry 4.0 (Smart Work Environment), is the new industrial revolution based on Cyber Physical Systems, where physical processes, workers and resources are monitored and a virtual copy of the physical environment is created to be processed and controlled by computer systems.



The Big Picture



Risk Management System

Knowledge

Monitoring

Analysis

Planning

Execution

Risk Events

Hazard

Risk Treatment

Preventive Strategies

Risk Description

Adaptive Security

Update the Attributes Based on Meta-rules

ACD Activated Based on Context

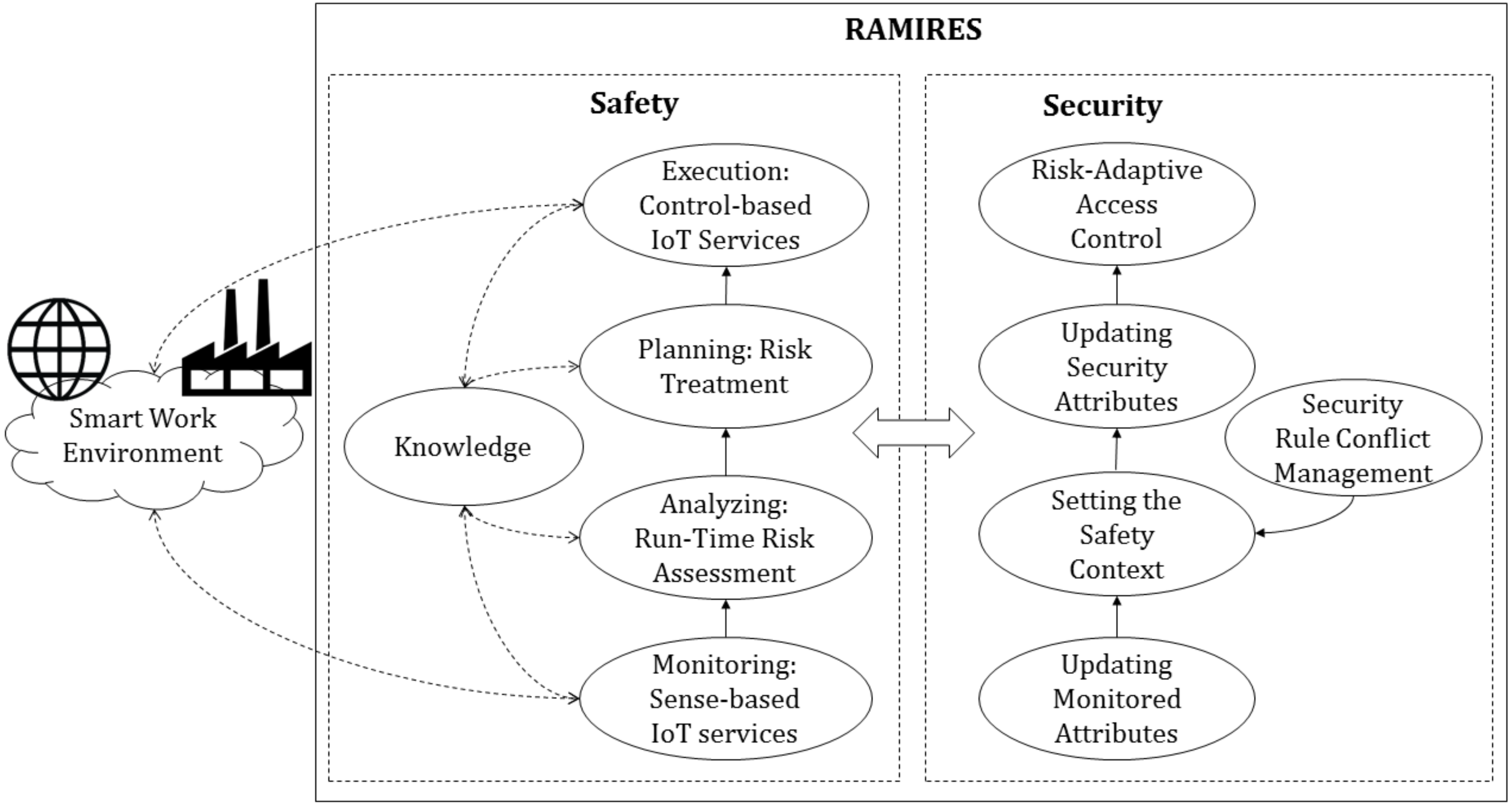
Adaptively Authorize Required Actions

Roll Back to the Safe Context

Receive Risk Description

Authorization

Co-Engineering Safety and Security: The Research Contributions



RAMIRES

Smart Work Environment

Safety

Execution: Control-based IoT Services

Planning: Risk Treatment

Knowledge

Analyzing: Run-Time Risk Assessment

Monitoring: Sense-based IoT services

Security

Risk-Adaptive Access Control

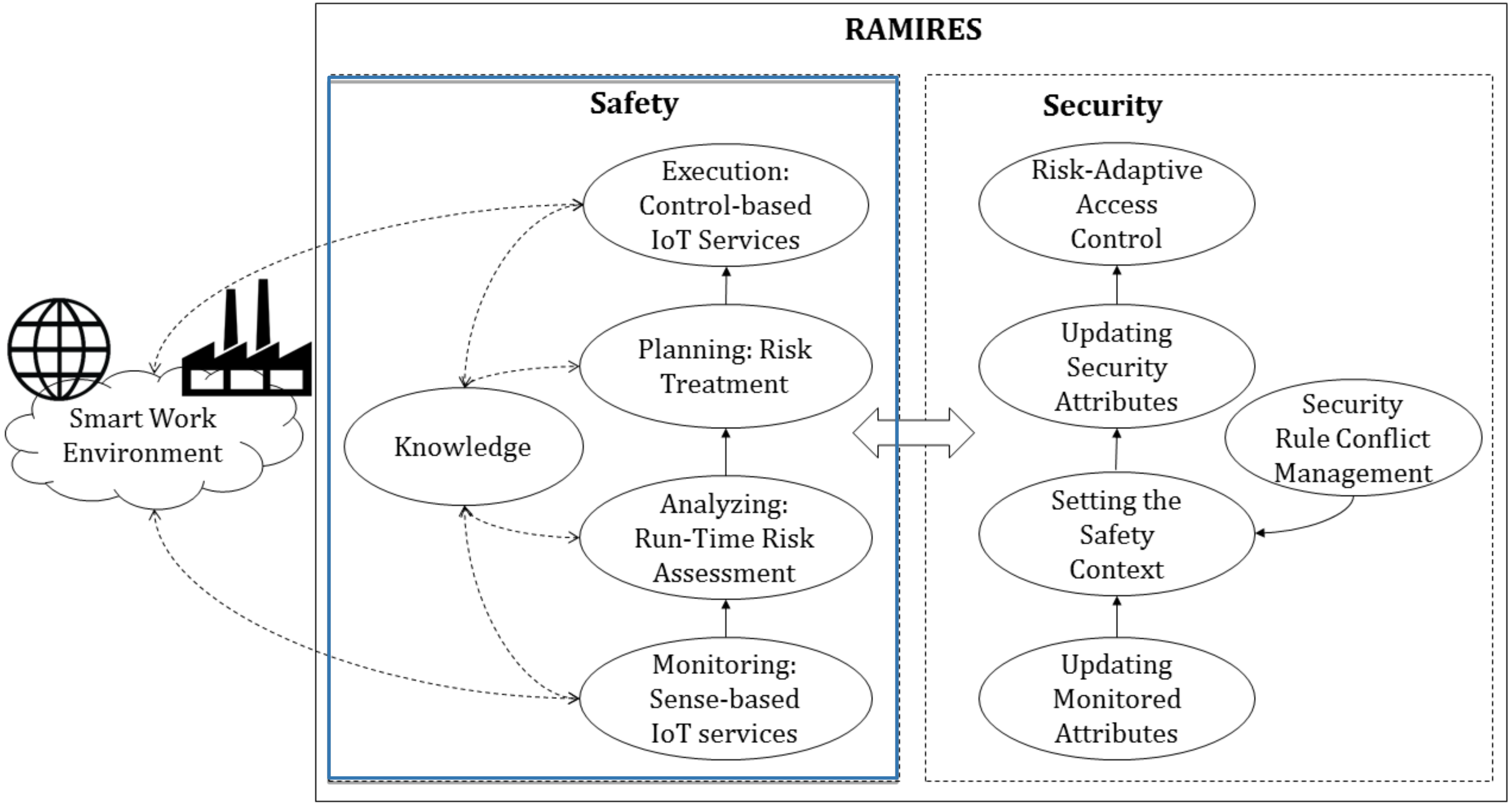
Updating Security Attributes

Security Rule Conflict Management

Setting the Safety Context

Updating Monitored Attributes

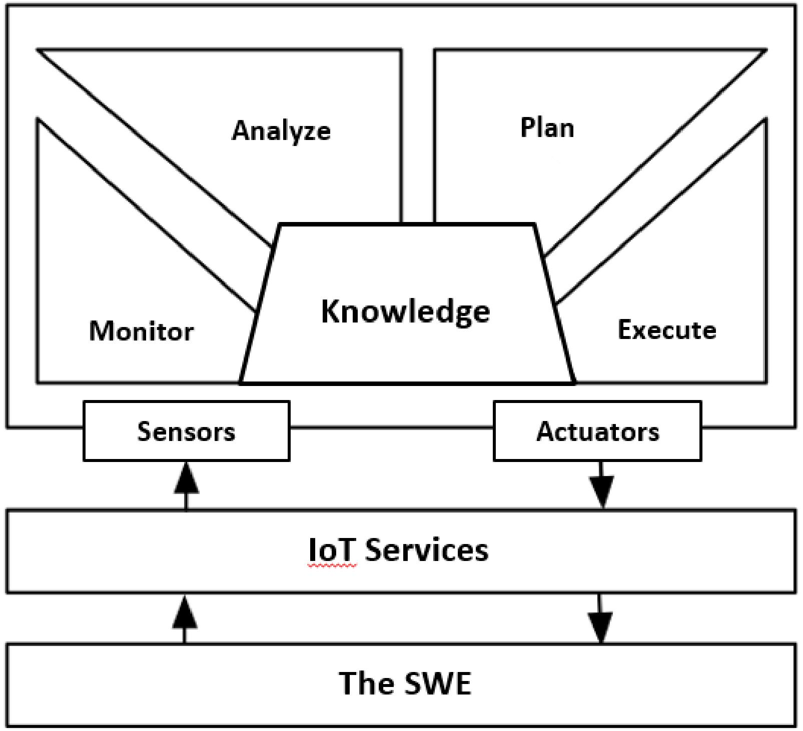
Co-Engineering Safety and Security: The Research Contributions


RAMIRES
Safety
Execution: Control-based IoT Services
Planning: Risk Treatment
Knowledge
Analyzing: Run-Time Risk Assessment
Monitoring: Sense-based IoT services
Smart Work Environment
Security
Risk-Adaptive Access Control
Updating Security Attributes
Security Rule Conflict Management
Setting the Safety Context
Updating Monitored Attributes

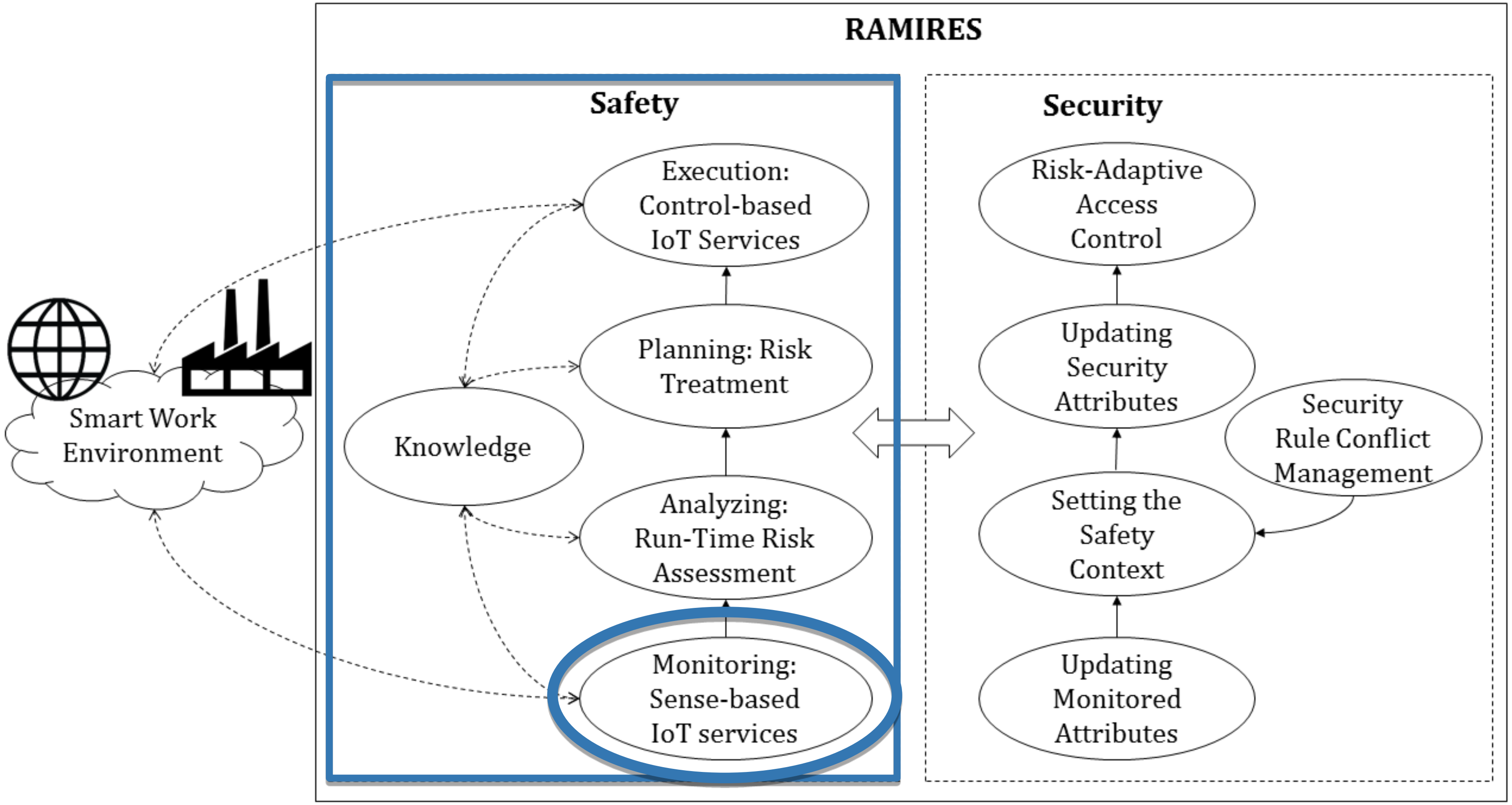
Run-Time Risk Management Methodology: MAPE-K Pattern Considering ISO 31000:2009

The MAPE-K Pattern:

- **Monitor:** is the process in which relevant elements in the environment are observed to signal a risk.
- **Analyze:** is the step where risk assessment should be conducted.
- **Plan:** concerns with the planning of preventive strategies
- **Execute:** has the goal of risk control that refers to the implementation of the risk treatment strategies.
- **Knowledge:** the safety knowledge represented using an ontology.

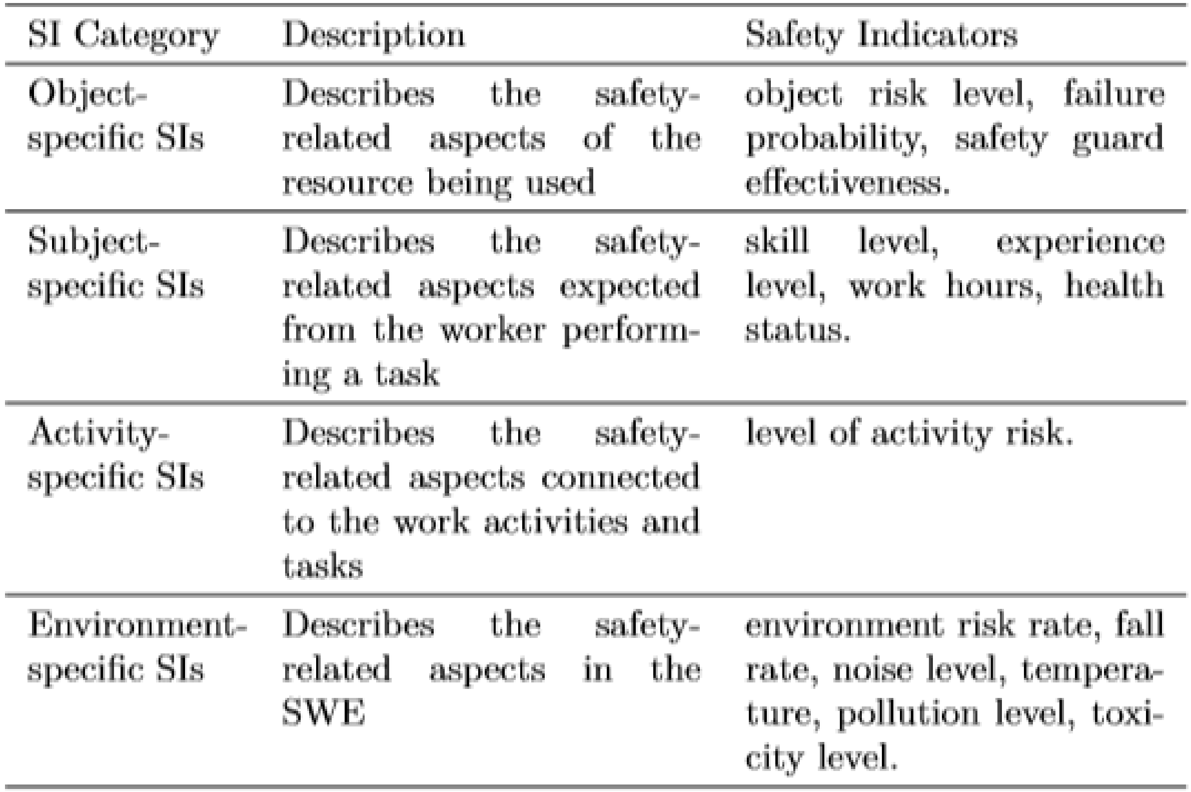


Co-Engineering Safety and Security: The research Contributions


RAMIRES
Safety
Execution: Control-based IoT Services
Planning: Risk Treatment
Knowledge
Analyzing: Run-Time Risk Assessment
Monitoring: Sense-based IoT services
Smart Work Environment
Security
Risk-Adaptive Access Control
Updating Security Attributes
Security Rule Conflict Management
Setting the Safety Context
Updating Monitored Attributes

Run-Time Risk Management Methodology: Monitor

- To define meaningful parameters to be monitored from the SWE Safety Indicators (SIs) are defined:



SI Category	Description	Safety Indicators
Object-specific SIs	Describes the safety-related aspects of the resource being used	object risk level, failure probability, safety guard effectiveness.
Subject-specific SIs	Describes the safety-related aspects expected from the worker performing a task	skill level, experience level, work hours, health status.
Activity-specific SIs	Describes the safety-related aspects connected to the work activities and tasks	level of activity risk.
Environment-specific SIs	Describes the safety-related aspects in the SWE	environment risk rate, fall rate, noise level, temperature, pollution level, toxicity level.

Run-Time Risk Management Methodology: Monitor

- The SWE *Safety Level (SL)* is a metric measuring the Safe/Unsafe status of a risk source based on the set of monitored *SIs*.
- Two methods are defined to calculate the SL of a risk source:
  - Range-based calculation method:

$$SL_t = \sum_{n>0} W_{P_n} \times f_n(SI_n)$$

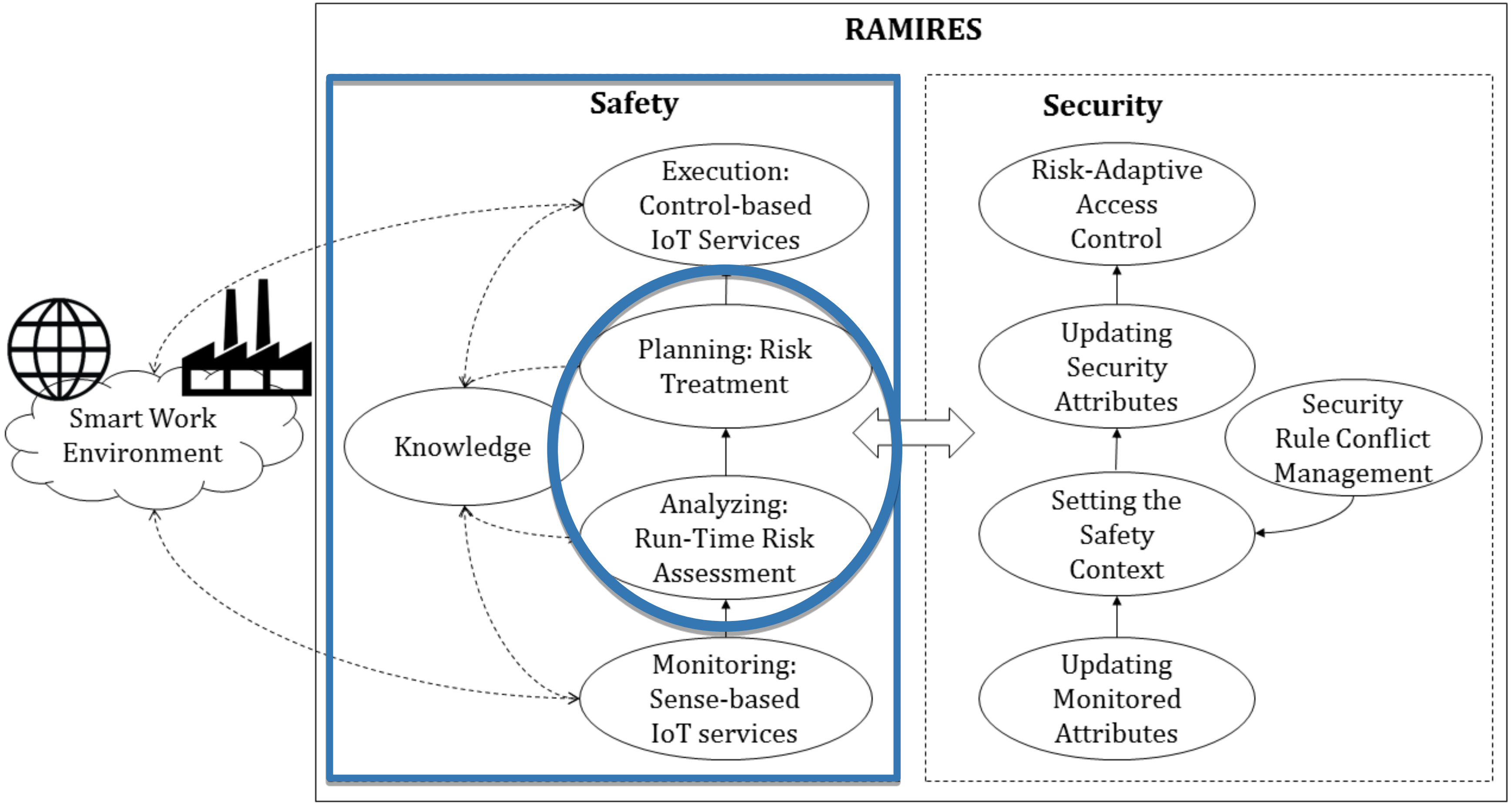
$$f_n(SI_n) = \begin{cases} 0, & if\ t_{min}(SI_n) \le value(SI_n) \le t_{max}(SI_n) \\ 1, & otherwise \end{cases}$$

  - Weight-based calculation method:

$$SL_w = \sum_{n>0} (W_{P_n} \times \frac{\sum_{j>0,i=n} W_{r_{ij}} \times V_{r_{ij}}}{\sum_{j>0,i=n} V_{r_{ij}}})$$

  - Where Vrnj is the deviation between the monitored value of the SI_i of entity j and its accepted value.

Co-Engineering Safety and Security: The research Contributions

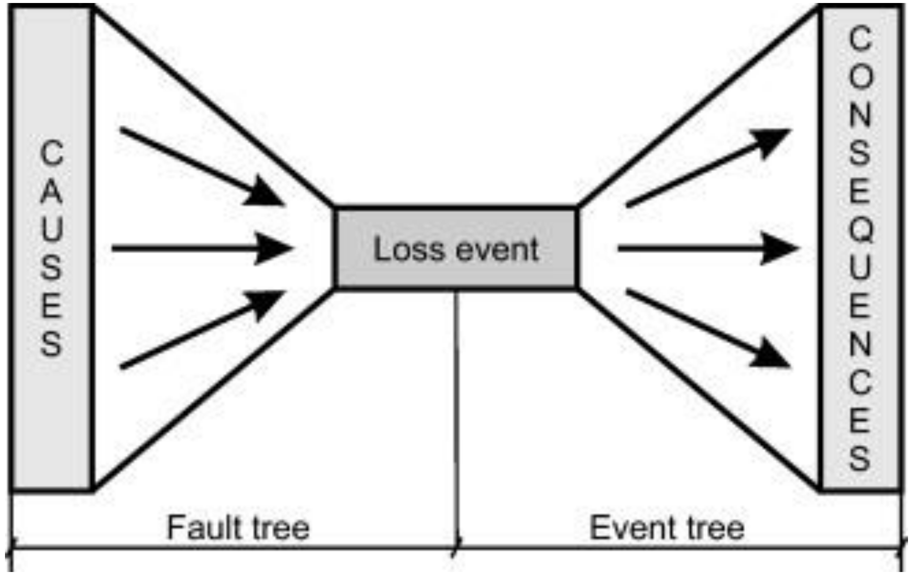

RAMIRES
Safety
Execution: Control-based IoT Services
Planning: Risk Treatment
Knowledge
Analyzing: Run-Time Risk Assessment
Monitoring: Sense-based IoT services
Smart Work Environment
Security
Risk-Adaptive Access Control
Updating Security Attributes
Security Rule Conflict Management
Setting the Safety Context
Updating Monitored Attributes

Modelling Operational Risk

- **Operational Risk** is the risk arising from an organization's business or operating functions. It covers people, processes, and systems that together or individually cause risk, whether these are external or internal to the organization.
- Analysis of operational risk recognizes that risk events are not solely to be blamed on human fallibility but are supported by organizational features that fail to defend against all-too-human mistakes, slips or malicious acts.
- In modelling operation risk, we consider people, process, and environment in addition to the hardware.

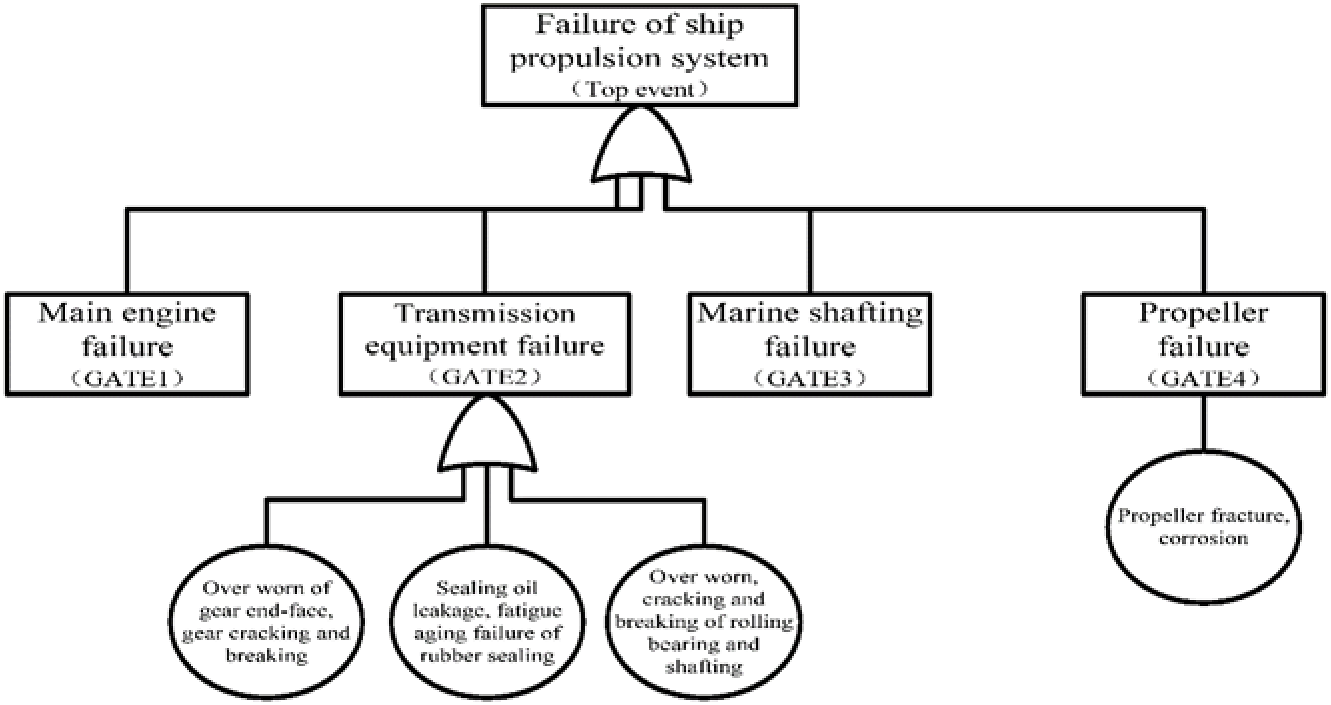
Bow Ties and Hazards

- Since hazards in conjunction with other events, can cause accidents it is crucial in a safety-related system to be able to identify, analyze, control and manage hazards.
- The two most important ways modelling safety and risk problems involving hazards are:
  - Causal models that lead to the hazard, called fault trees
  - Concequence models contingent on the hazard having occurred, called event trees



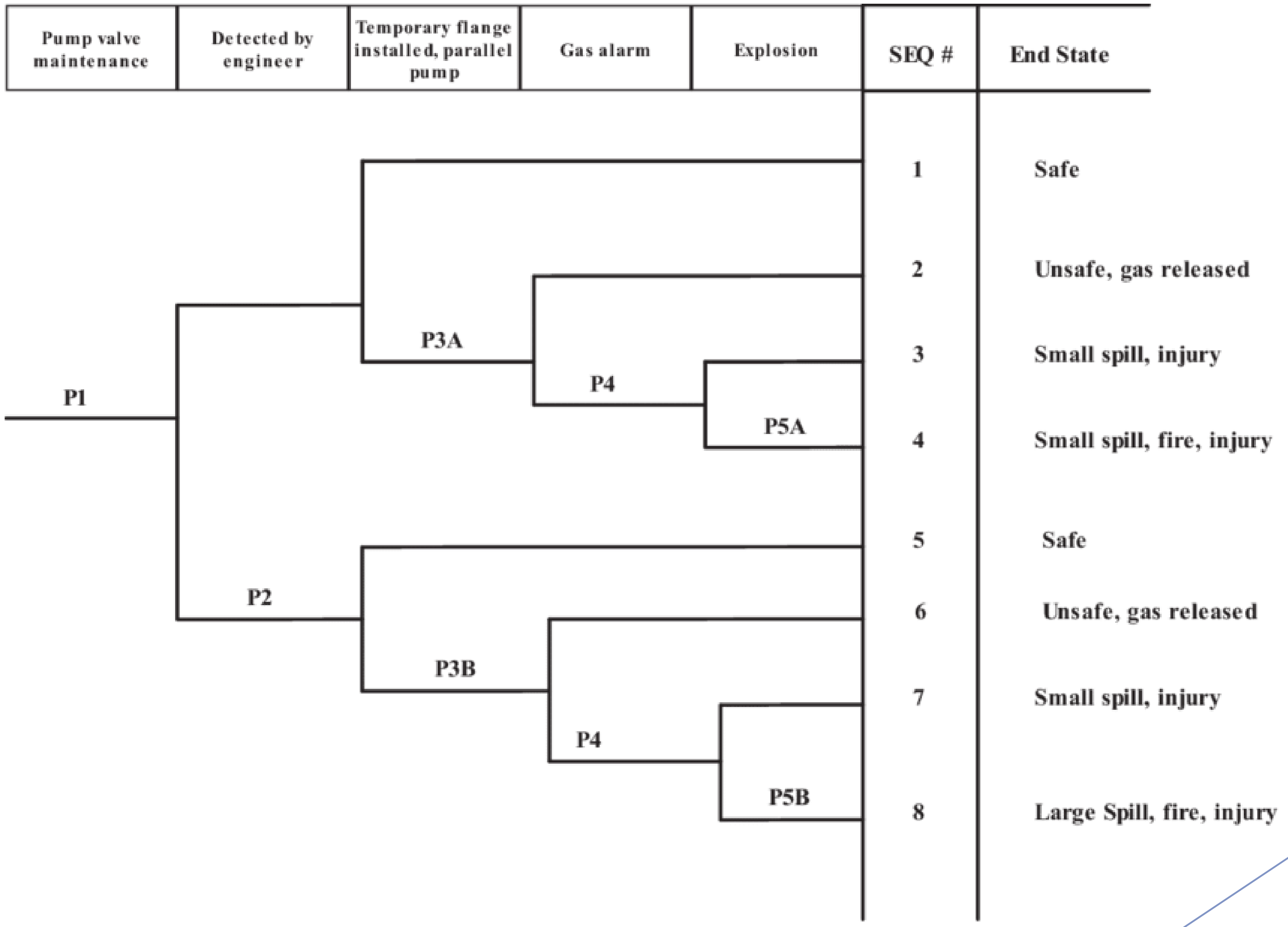
Fault-Tree Analysis (FTA)

- Example of a fault tree


Failure of ship propulsion system
（Top event）
Main engine failure
（GATE1）
Transmission equipment failure
（GATE2）
Marine shafting failure
（GATE3）
Propeller failure
（GATE4）
Over worn of gear end-face, gear cracking and breaking
Sealing oil leakage, fatigue aging failure of rubber sealing
Over worn, cracking and breaking of rolling bearing and shafting
Propeller fracture, corrosion

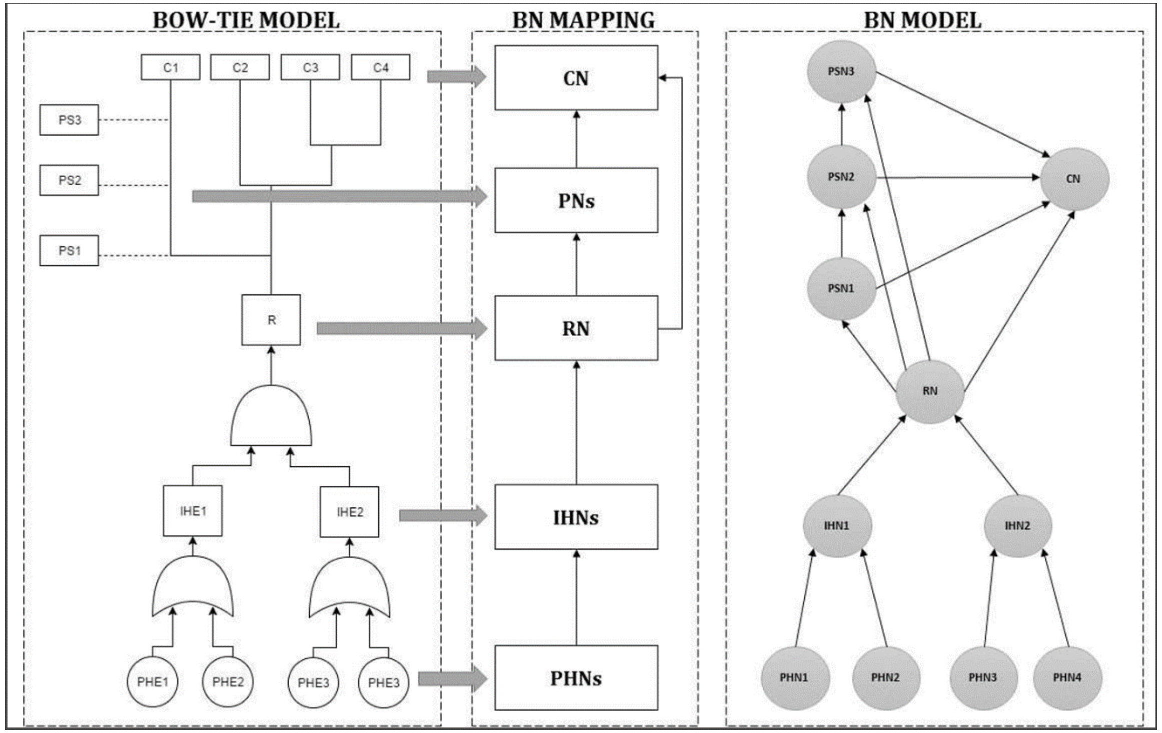
Event-Tree Analysis (ETA)

- Example of an event tree

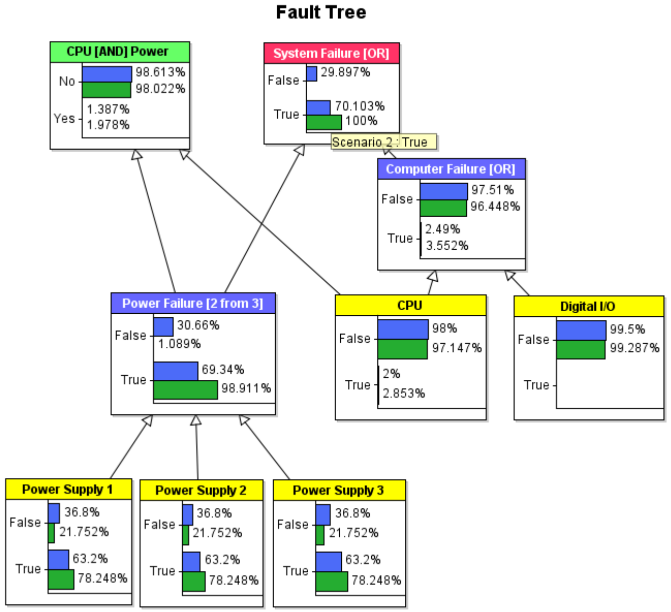


SEQ #	End State
1	Safe
2	Unsafe, gas released
3	Small spill, injury
4	Small spill, fire, injury
5	Safe
6	Unsafe, gas released
7	Small spill, injury
8	Large Spill, fire, injury

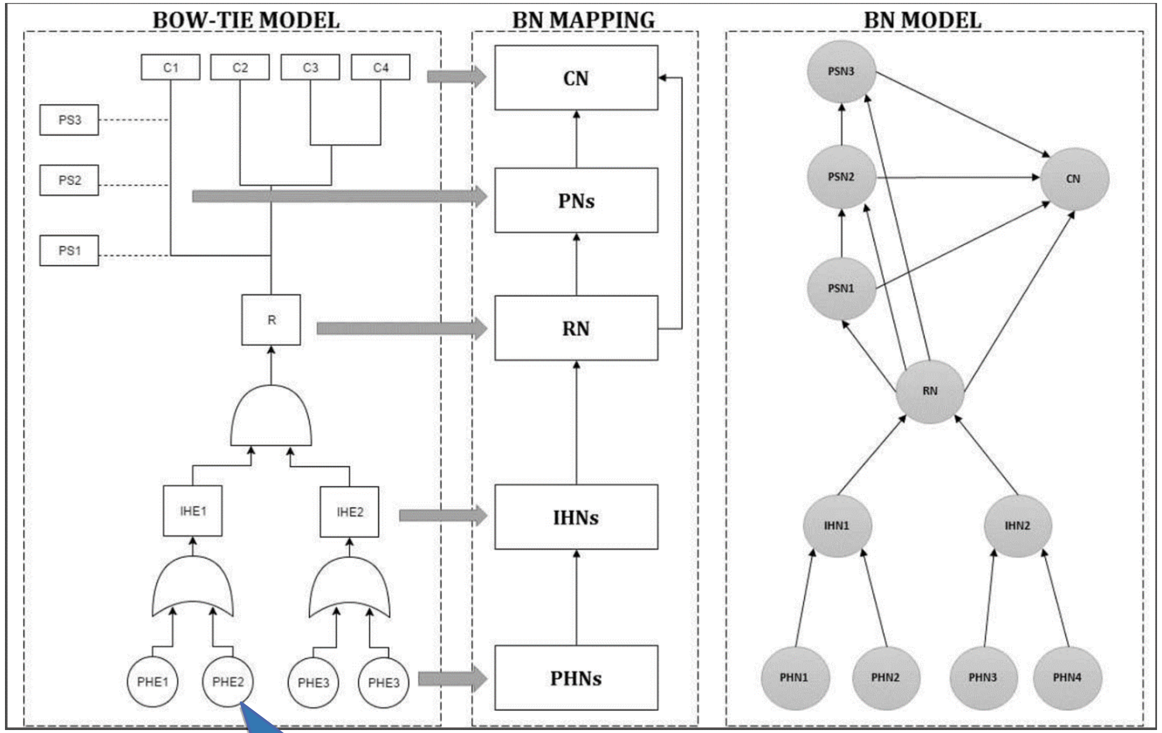
Run-Time Risk Management Methodology: Analyze and Plan



- The Bow-Tie Model is mapped into Bayesian Networks for automated Risk Assessment.

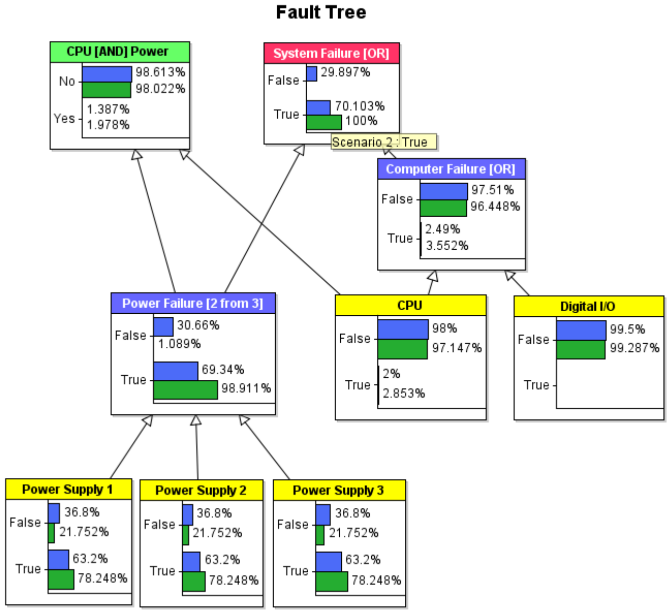


Run-Time Risk Management Methodology: Analyze and Plan

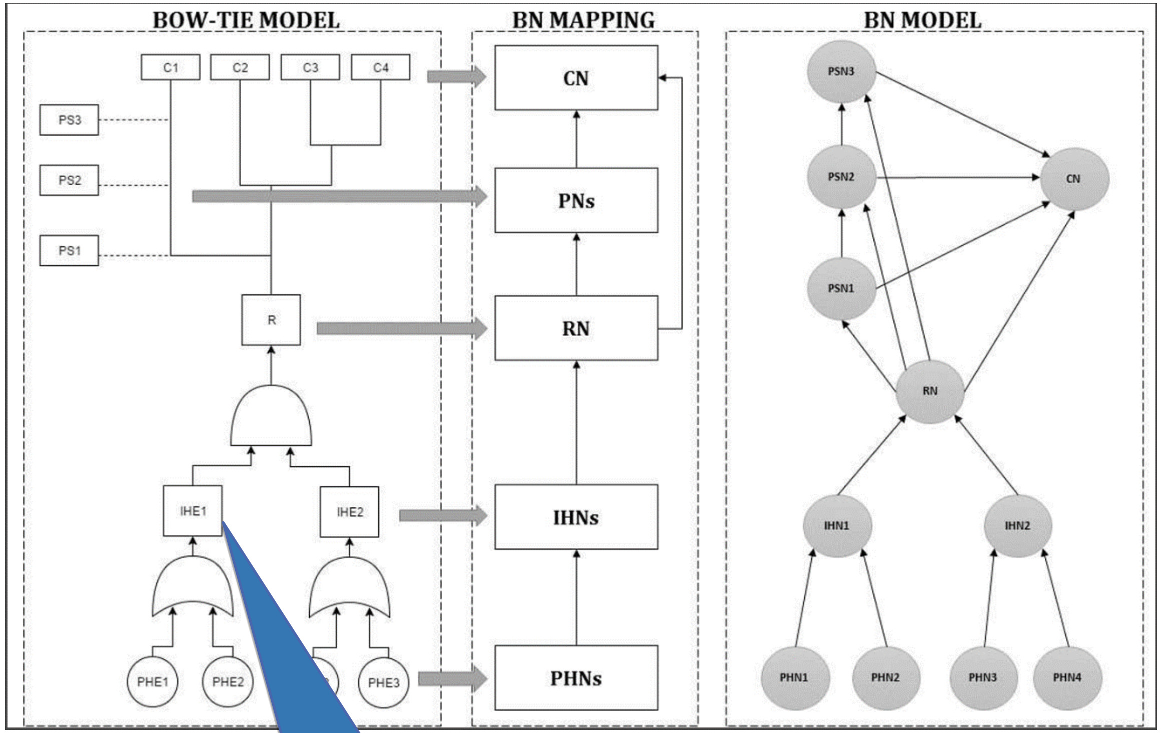


Primary
Hazardous Events

- The Bow-Tie Model is mapped into Bayesian Networks for automated Risk Assessment.

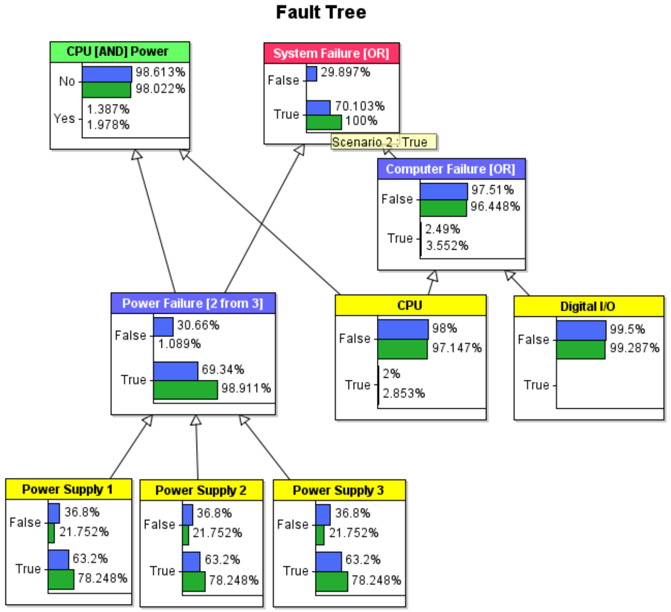


Run-Time Risk Management Methodology: Analyze and Plan

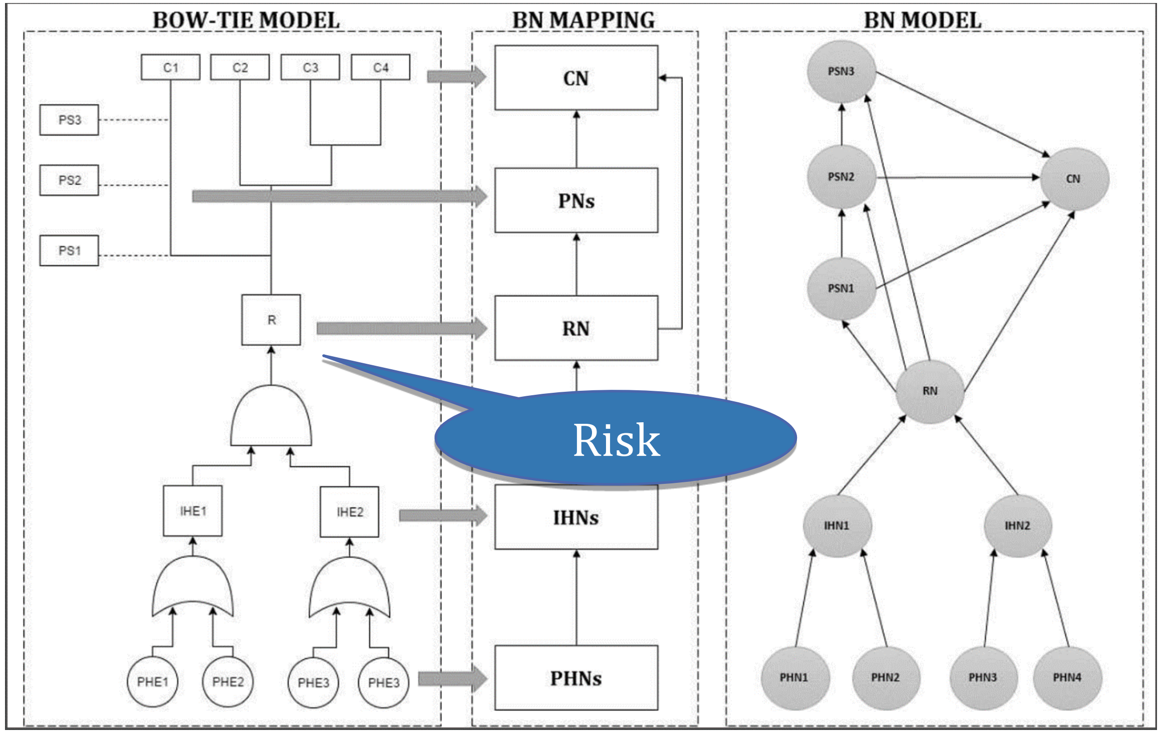


Intermediate Hazardous Events

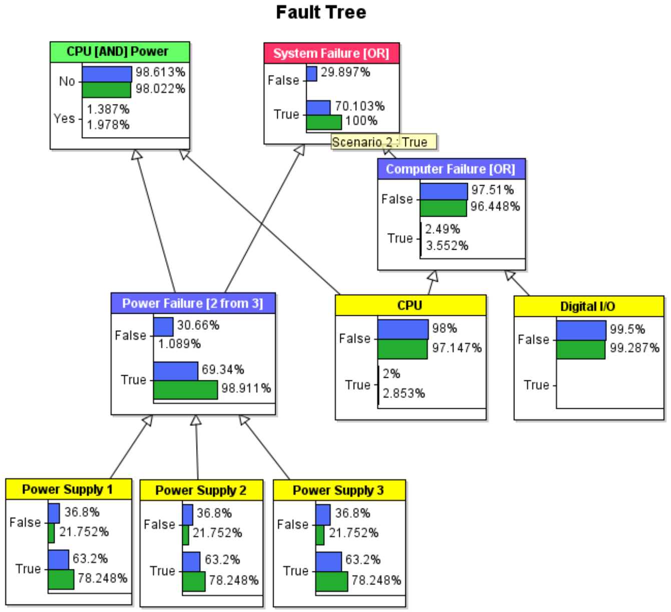
- The Bow-Tie Model is mapped into Bayesian Networks for automated Risk Assessment.



Run-Time Risk Management Methodology: Analyze and Plan



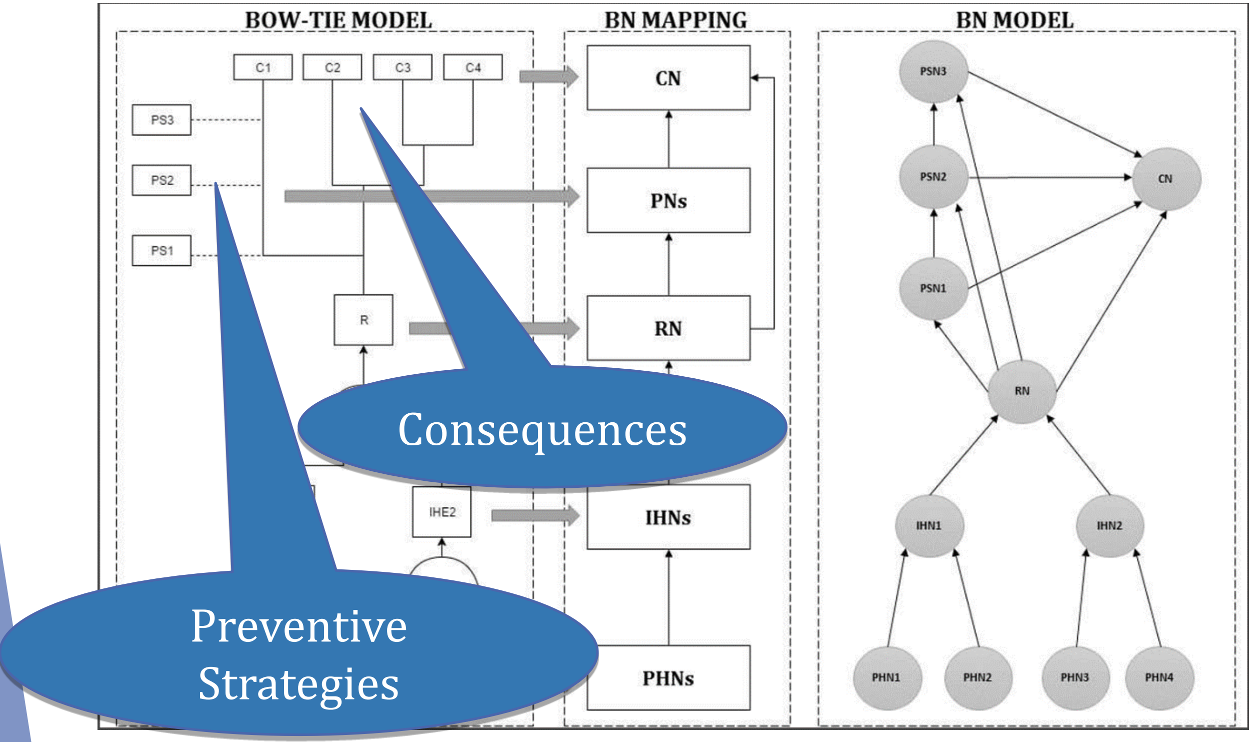
- The Bow-Tie Model is mapped into Bayesian Networks for automated Risk Assessment.



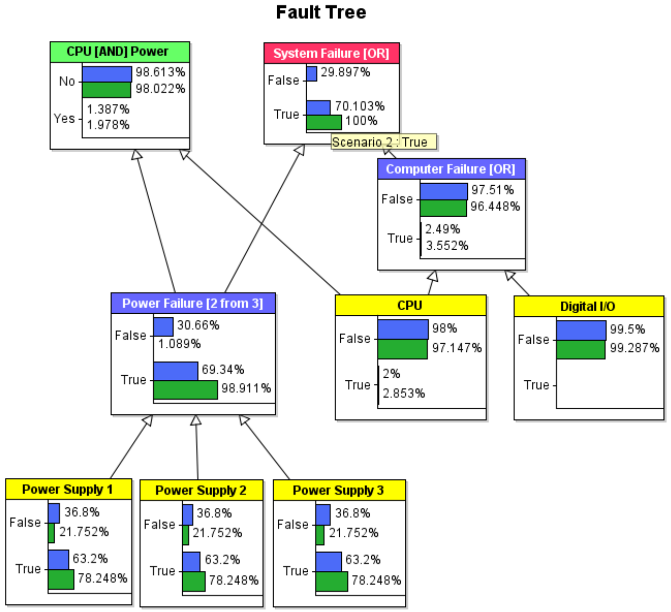
Transforming the fault-tree into the Bayesian Networks

- the *Primary Hazardous Events (PHEs)*, *Intermediate Hazardous Events (IHEs)* and the *Risk (R)* in the Fault-Tree are represented as nodes in the BN.
- the fundamental arrows between the BN nodes are produced based on their relationships that are defined in the Fault-Tree.
- Later, based on safety experts opinions further arrows are added to denote the supplementary causal relationships between hazardous events.
- To measure the correlation of child nodes to their connected parents in the transformed BT model, weights are considered that are defined by safety experts.
    - Using weight functions it is possible to include the effects of logical *AND/OR* gates in the transformed Fault-Tree.

Run-Time Risk Management Methodology: Analyze and Plan



- The Bow-Tie Model is mapped into Bayesian Networks for automated Risk Assessment.



Transforming the Event-Tree into the Bayesian Networks

- Each *Preventive Strategy (PS)* is represented by a *PS node (PSN)* in the BN having two states of failure and success.
- A *Consequence Node (CN)* is defined having the states of different consequences in the original Event-Tree (e.g., {*C*1, ...,*C*4})
- In this approach, PS node *PSNi* is connected to its previous node *PSNi*−1 that represents the preceding preventive strategy, having the condition that, the probability of failure or success of *PSNi* depends on whether *PSNi*−1 has been performed successfully or not. In other words, these two nodes are connected only if:

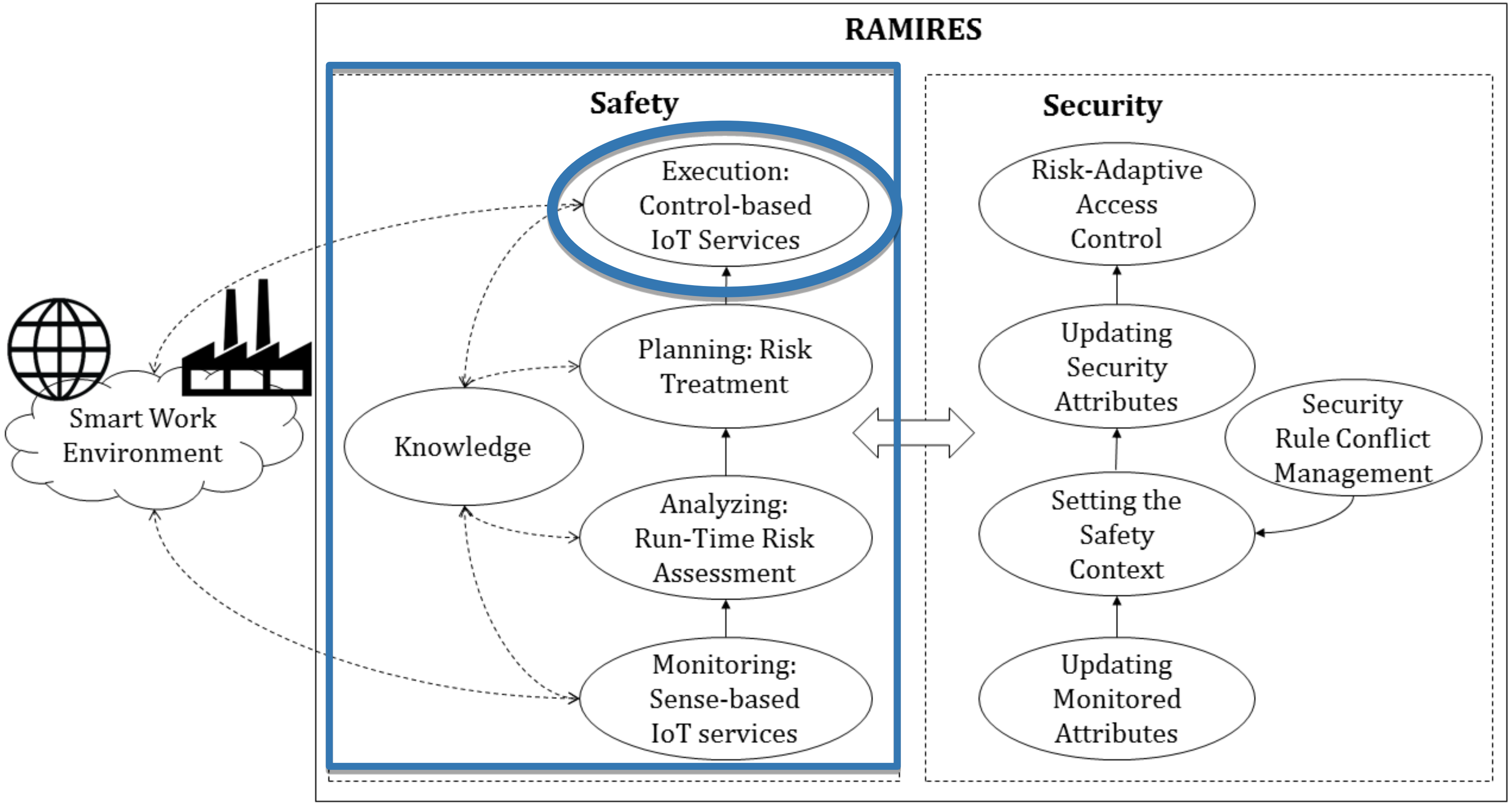
$$P(PSN_i|PSN_{i-1}) \neq P(PSN_i|\overline{PSN_{i-1}})$$

- Furthermore, considering the Consequence node *CNi*, any *PSNj* should have a link to *CNi* only if:

$$P(CN_i|PSN_j) \neq P(CN_i|\overline{PSN_j})$$

- meaning that the probabilities of the states of (*CNi*) depend on (are affected by) the success or failure of *PSNj* .

Co-Engineering Safety and Security: The research Contributions



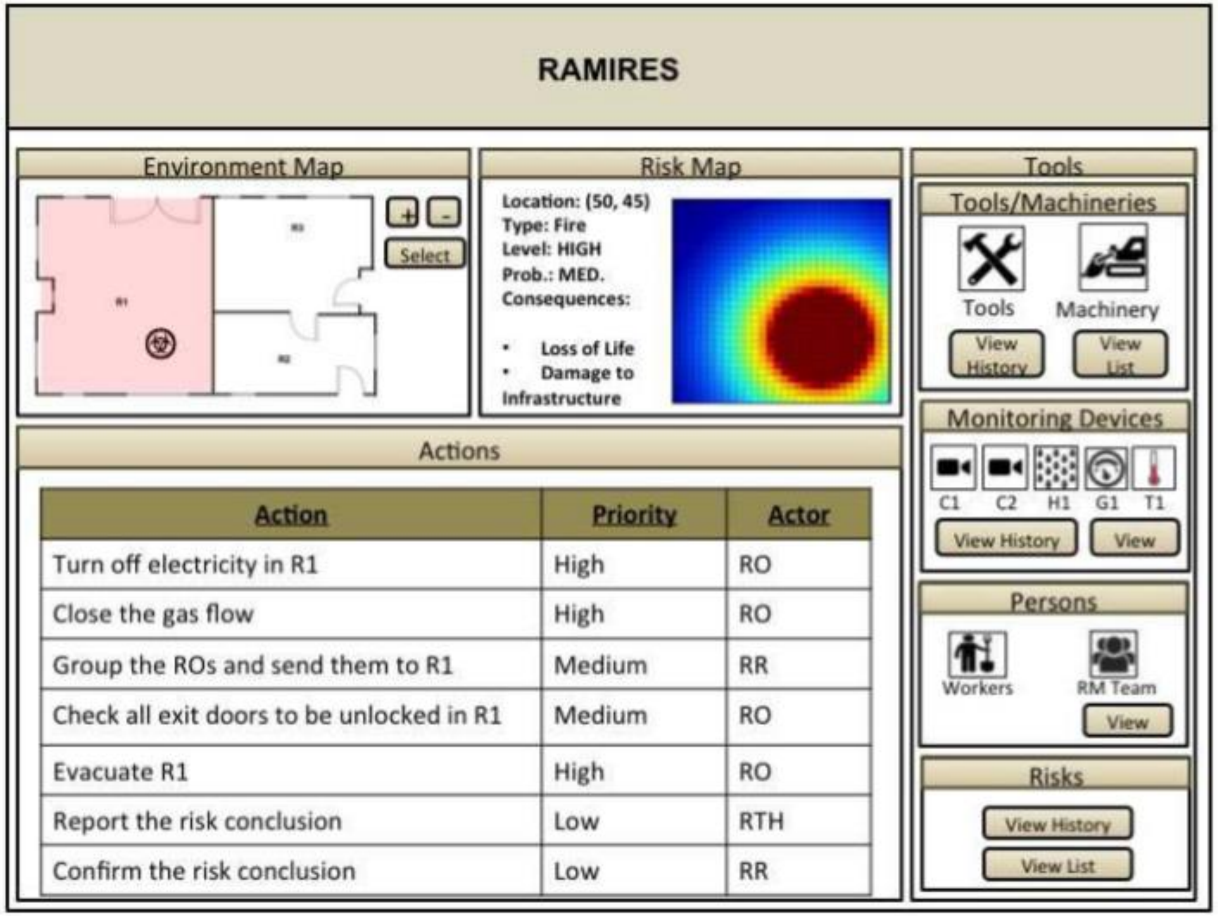
RAMIRES
Safety
Execution: Control-based IoT Services
Planning: Risk Treatment
Knowledge
Analyzing: Run-Time Risk Assessment
Monitoring: Sense-based IoT services
Smart Work Environment
Security
Risk-Adaptive Access Control
Updating Security Attributes
Security Rule Conflict Management
Setting the Safety Context
Updating Monitored Attributes

Run-Time Risk Management Methodology: Execute

Execute the preventive strategies:

- **Automated strategies:** Using Control-Based IoT-Services
- **Human-operated strategies:** Communicated using a dashboard.

- The security system indicates which information should be shown to which user based on the defined rules. (This will be explained later on)



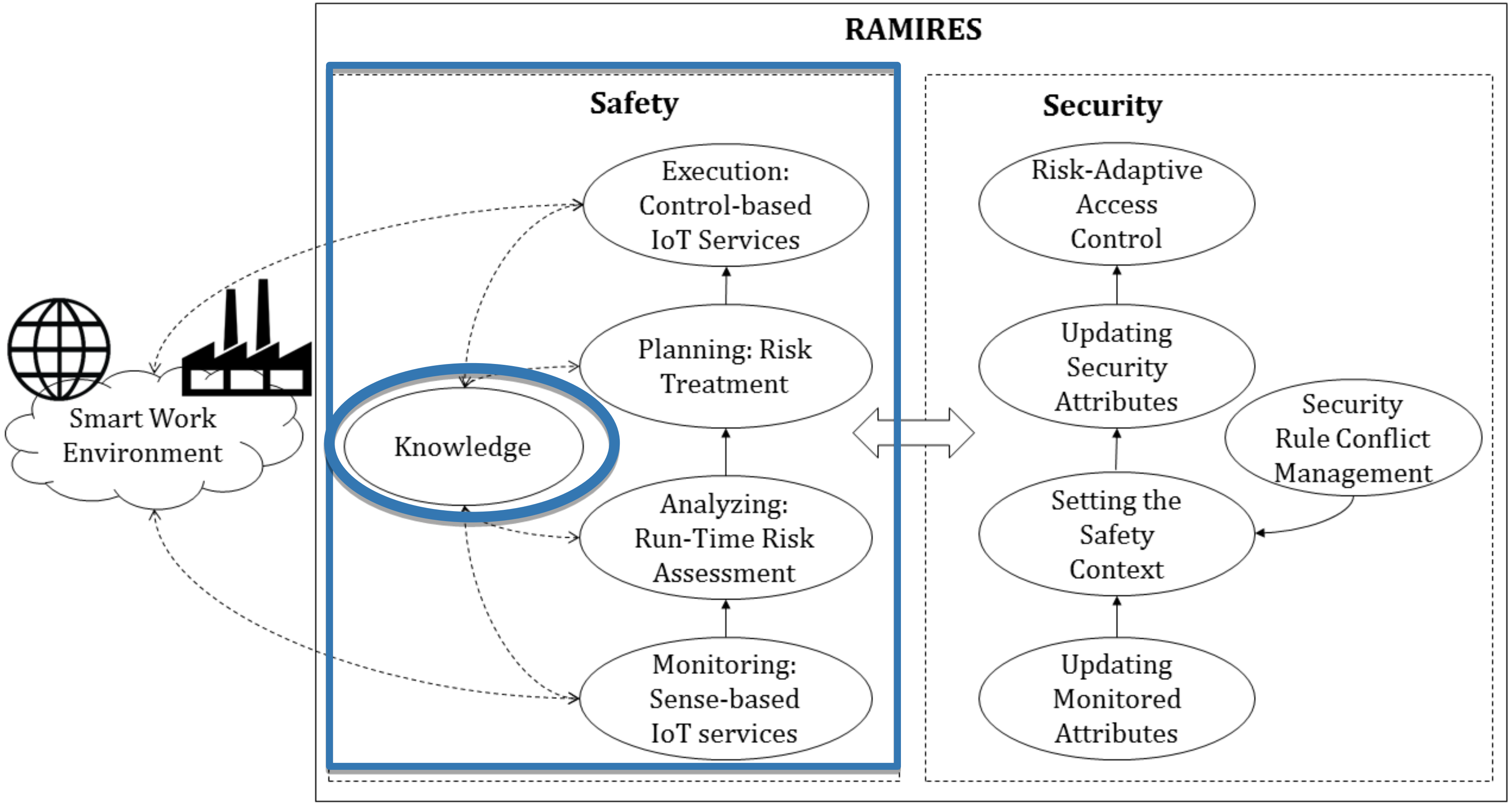
RAMIRES

Location: (50, 45)
Type: Fire
Level: HIGH
Prob.: MED.
Consequences:
- Loss of Life
- Damage to Infrastructure

Actions

Action	Priority	Actor
Turn off electricity in R1	High	RO
Close the gas flow	High	RO
Group the ROs and send them to R1	Medium	RR
Check all exit doors to be unlocked in R1	Medium	RO
Evacuate R1	High	RO
Report the risk conclusion	Low	RTH
Confirm the risk conclusion	Low	RR

Co-Engineering Safety and Security: The research Contributions

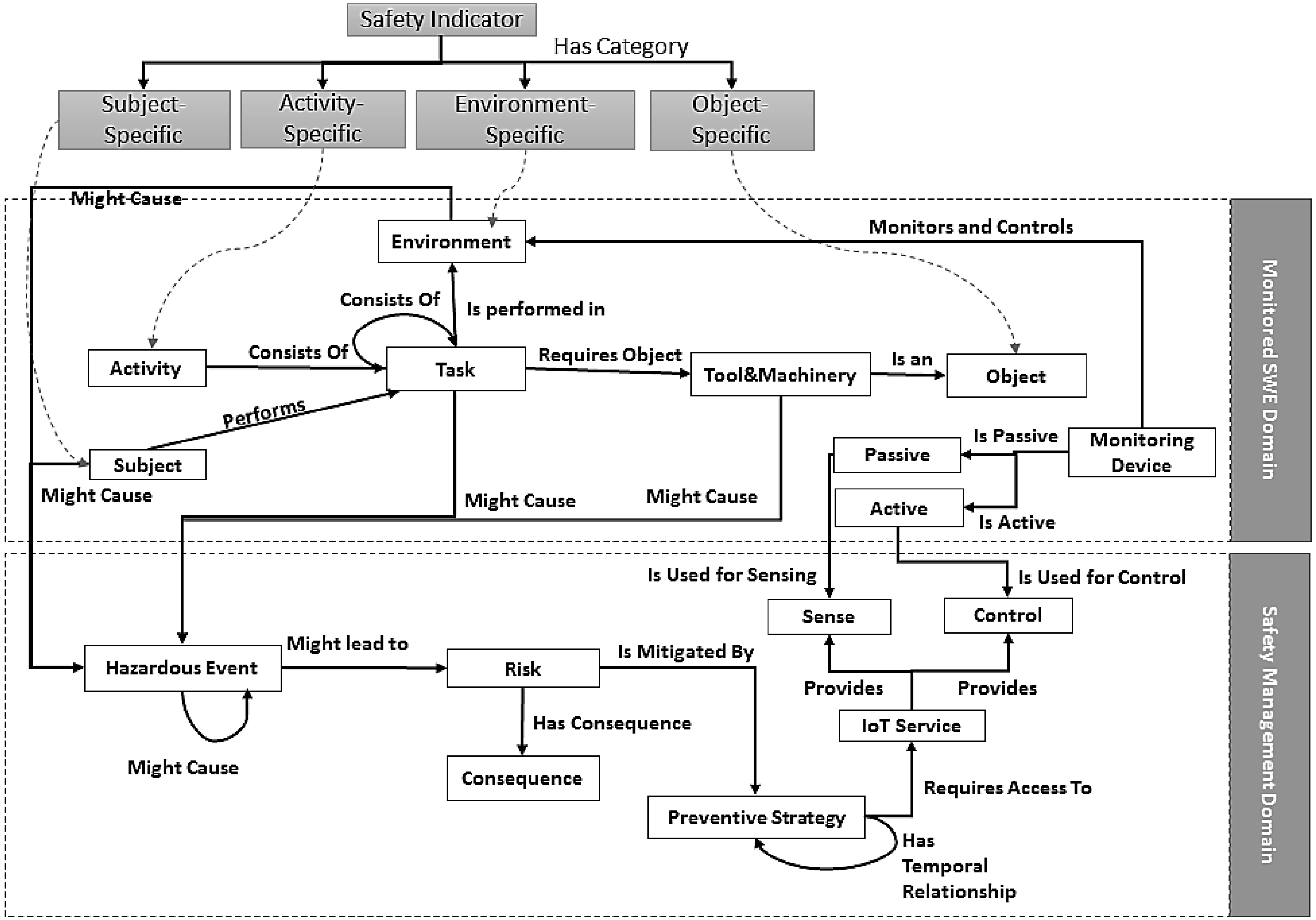


RAMIRES
Safety
Execution: Control-based IoT Services
Planning: Risk Treatment
Knowledge
Analyzing: Run-Time Risk Assessment
Monitoring: Sense-based IoT services
Smart Work Environment
Security
Risk-Adaptive Access Control
Updating Security Attributes
Security Rule Conflict Management
Setting the Safety Context
Updating Monitored Attributes

Run-Time Risk Management Methodology: Knowledge

Ontologies are used to represent the knowledge in the MAPE-K Pattern.

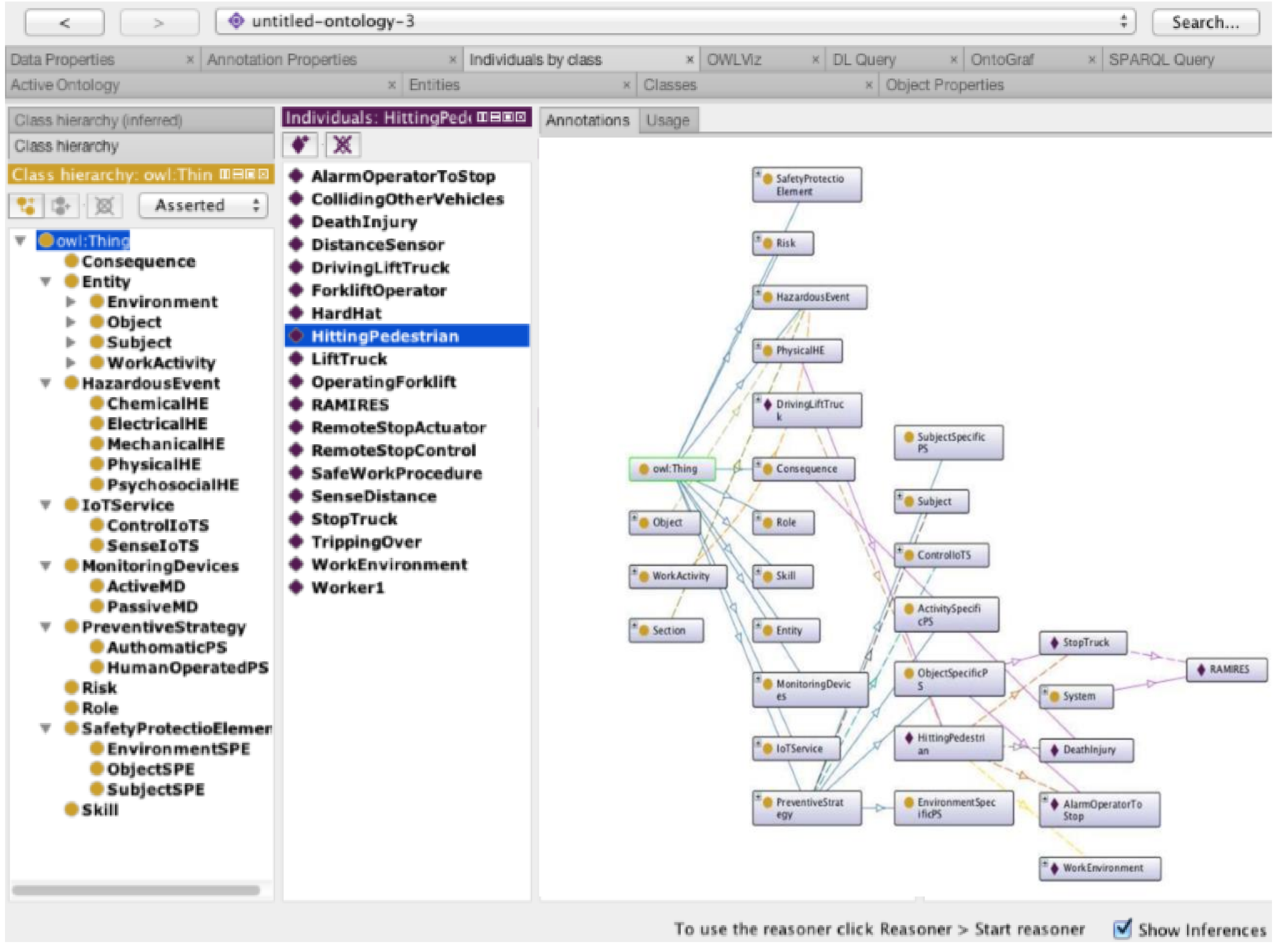
The designed ontology includes the Monitored and the Safety domains.



The Safety Knowledge

The Ontology is developed on Protégé.

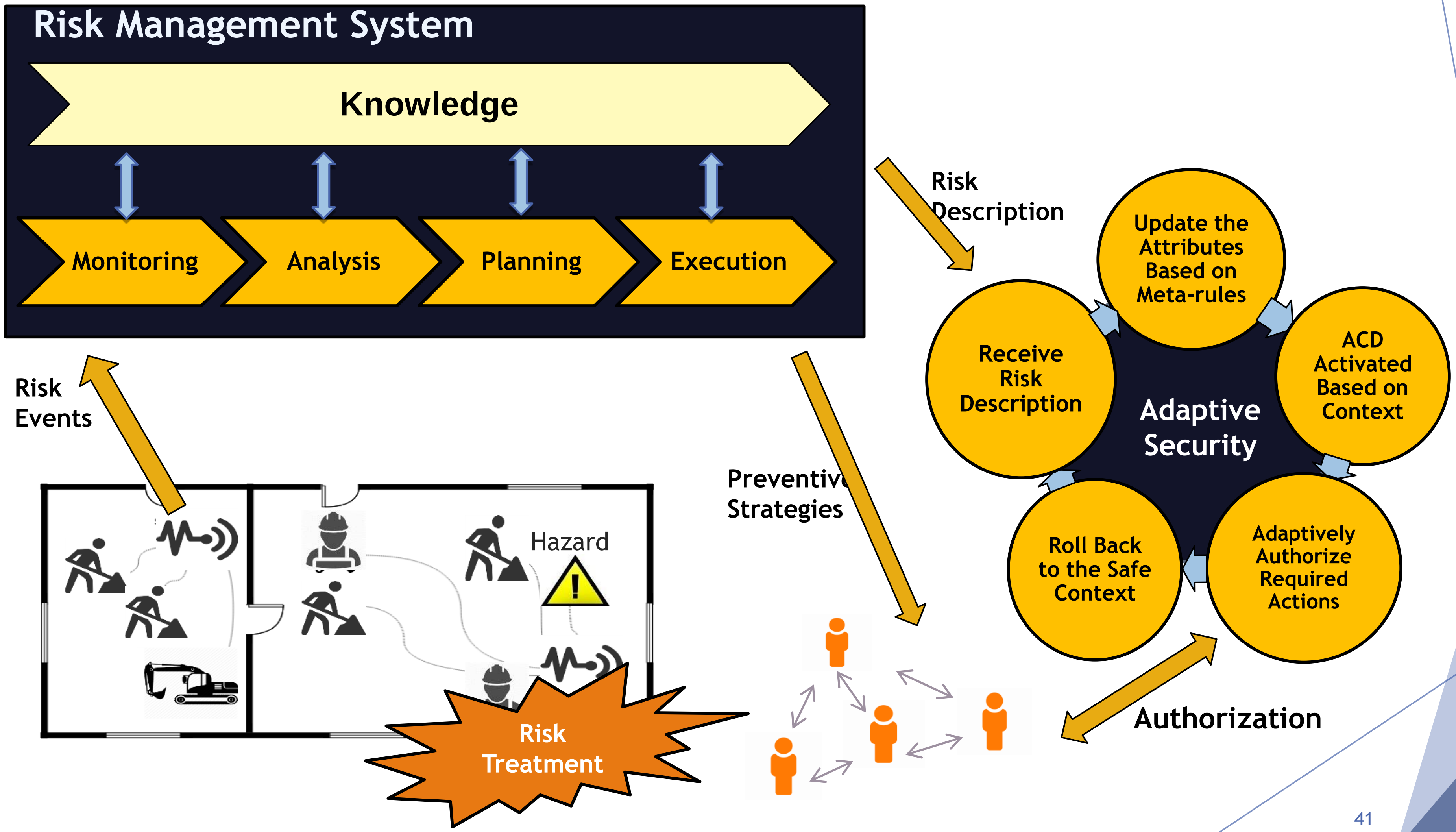
A Description Logic (DL) reasoner called HermiT is used to automatically check the formal consistency of the ontology and to verify that it is minimally redundant.



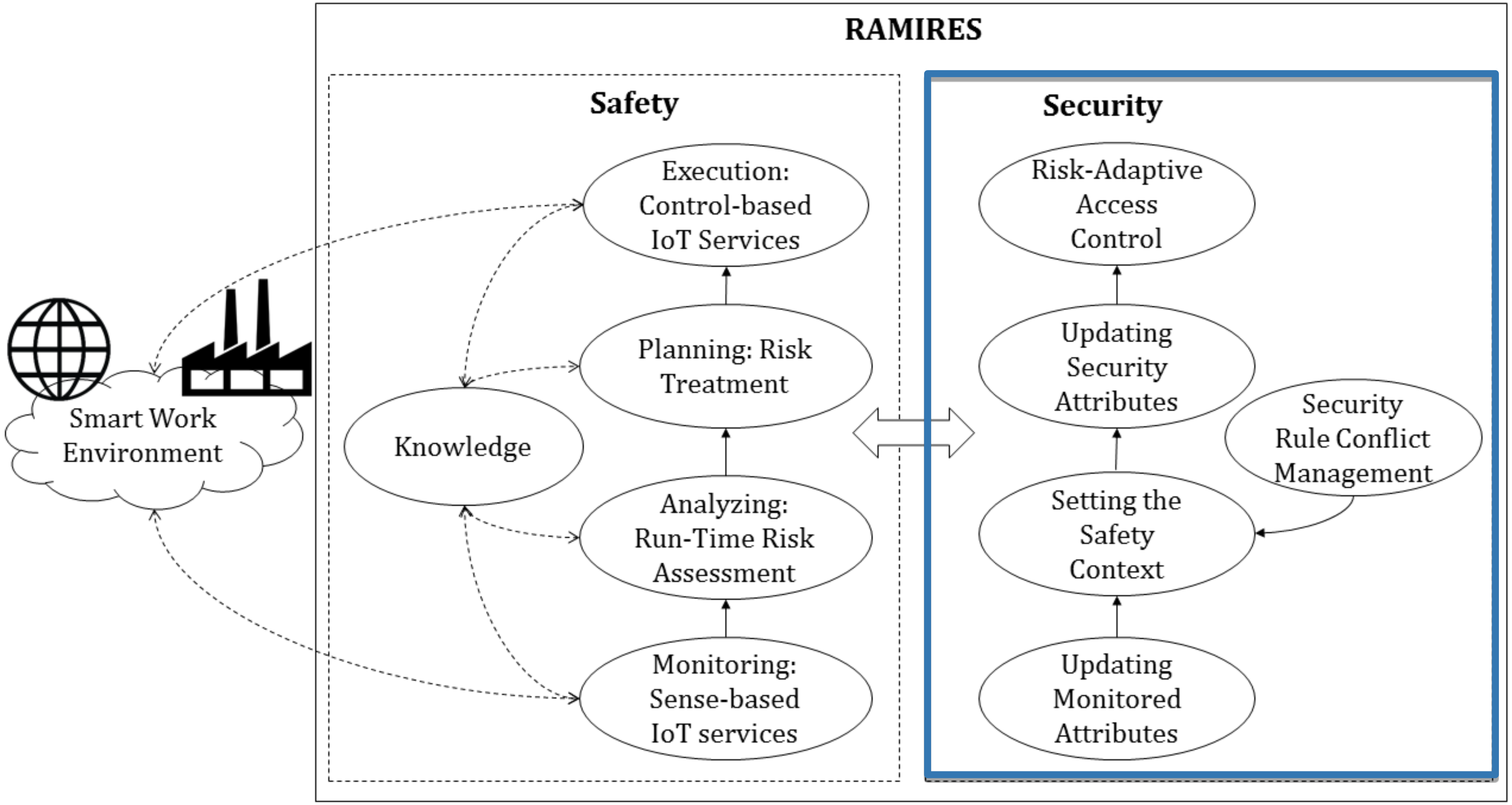
To use the reasoner click Reasoner > Start reasoner

☑ Show Inferences

The Big Picture



Co-Engineering Safety and Security: The research Contributions


RAMIRES
Safety
Security
Smart Work Environment
Knowledge
Execution: Control-based IoT Services
Planning: Risk Treatment
Analyzing: Run-Time Risk Assessment
Monitoring: Sense-based IoT services
Risk-Adaptive Access Control
Updating Security Attributes
Security Rule Conflict Management
Setting the Safety Context
Updating Monitored Attributes

Risk-Adaptive Access Control: Security Rules

- Security rules in the AC model are defined as follows:

$$\begin{aligned} ru_i \rightarrow & \textbf{ON} :< Target > \\ & \textbf{IF} :< Condition > \\ & \textbf{THEN} :< Effect > \end{aligned}$$

- Where:

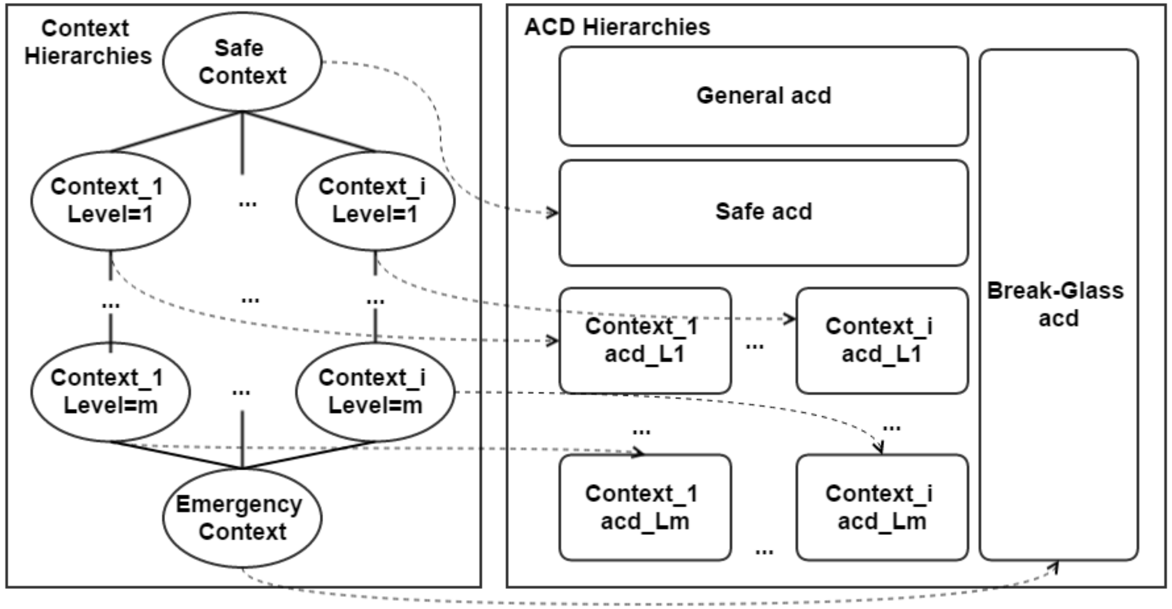
- *Target* is a logical statement that indicates if the security rule is a match for a specific request or not.
- *Condition* defines the set of attributes and their values leading to the specified *authorization decision*
- *Effect* is the result of the *authorization decision*, which can get the values: *Permit* or *Deny.*

- An example of a security rule is given below:

$$\begin{aligned} ru_1 \rightarrow & \textbf{ON} : p = \text{“}ActivateAlarm\text{”} \\ & \textbf{IF} : en.Pollution > SafePollutionLevel \\ & \wedge s.Role = \text{“}SafetyStaff\text{”} \\ & \wedge o.Type = \text{“}EvacuationAlarm\text{”} \\ & \textbf{THEN} : \text{“}Permit\text{”} \end{aligned}$$

Risk-Adaptive Access Control: Setting the Safety Contexts

- *Access Control Domains (ACDs)* are sets of security rules that are designed for specific safety situations evaluated by the risk management system.
- An *ACD* allows to enforce the security rules that allow risk treatment for specific types of *global risks (R_global)* with various levels of intensity.



- To introduce context-awareness to the ABAC model, hierarchical safety-related contexts are defined with different levels of intensity which are mapped to related ACDs

Risk-Adaptive Access Control: Setting the Safety Contexts

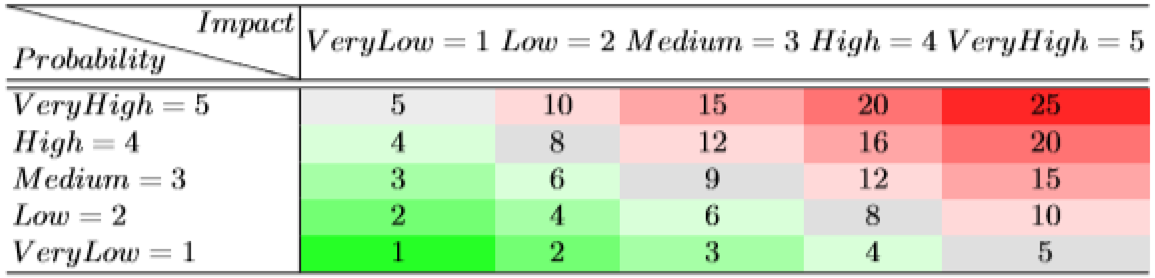
- The risk description is received from the risk management system:

$$rd_i = \{r_i.Type, r_i.Probability, r_i.Source, r_i.Location, r_i.C_{ri}\}$$

- Each context represents the type of the risk (*ri.Type*) e.g., fire.
- To calculate the level of the criticality:

$$context_i.level = RiskLevel(r_i) = r_i.Probability \times r_i.Severity$$

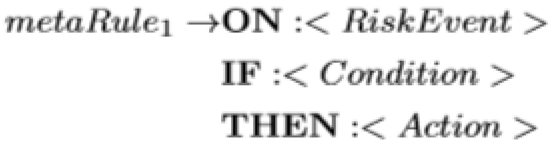
  - *Severity* is calculated by safety experts, considering the costs that the risk consequences have for the specific organization.



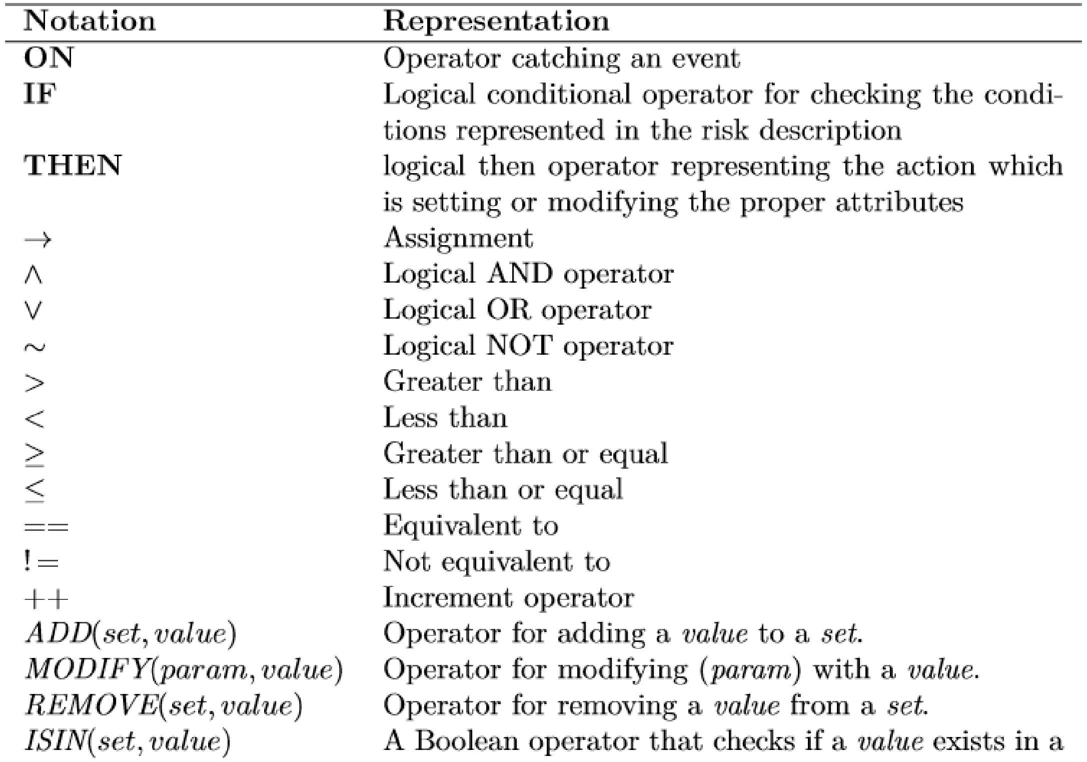
$Impact$ $Probability$	$VeryLow = 1$	$Low = 2$	$Medium = 3$	$High = 4$	$VeryHigh = 5$
$VeryHigh = 5$	5	10	15	20	25
$High = 4$	4	8	12	16	20
$Medium = 3$	3	6	9	12	15
$Low = 2$	2	4	6	8	10
$VeryLow = 1$	1	2	3	4	5

Risk-Adaptive Access Control: Meta-Rules

- **Event-Condition-Action (ECA) meta-rules are defined for dynamically adapting the security policies.** A formal notation is introduced to formally define these meta-rules.



$$\begin{aligned} metaRule_1 \rightarrow & \textbf{ON} :< RiskEvent > \\ & \textbf{IF} :< Condition > \\ & \textbf{THEN} :< Action > \end{aligned}$$



Notation	Representation
ON	Operator catching an event
IF	Logical conditional operator for checking the conditions represented in the risk description
THEN	logical then operator representing the action which is setting or modifying the proper attributes
$\rightarrow$	Assignment
$\wedge$	Logical AND operator
$\vee$	Logical OR operator
$\sim$	Logical NOT operator
$>$	Greater than
$<$	Less than
$\geq$	Greater than or equal
$\leq$	Less than or equal
$==$	Equivalent to
$!=$	Not equivalent to
$++$	Increment operator
$ADD(set, value)$	Operator for adding a *value* to a *set*.
$MODIFY(param, value)$	Operator for modifying (*param*) with a *value*.
$REMOVE(set, value)$	Operator for removing a *value* from a *set*.
$ISIN(set, value)$	A Boolean operator that checks if a *value* exists in a

Risk-Adaptive Access Control: Examples of Meta-Rules

Examples of meta-rules for managing safety related contexts:

- Adding a new context:

$$\begin{aligned} metaRule_1 \rightarrow & \textbf{ON} : ReceivedGlobalRisk(r) \wedge ReceivedContext(context_{data}) \\ & \textbf{IF} : context.level \leq T_{emergency} \wedge r.context.level \geq T_{safe} \\ & \textbf{THEN} : ADD(ContextList, [context, context.level]) \end{aligned}$$

- Setting the Emergency Context:

$$\begin{aligned} metaRule_2 \rightarrow & \textbf{ON} : ReceivedGlobalRisk(r) \wedge ReceivedContext(context_{data}) \\ & \textbf{IF} : context.level \geq T_{emergency} \\ & \textbf{THEN} : REMOVE(ContextList, ALL) \\ & \wedge MODIFY(EmergencyContext, TRUE) \end{aligned}$$

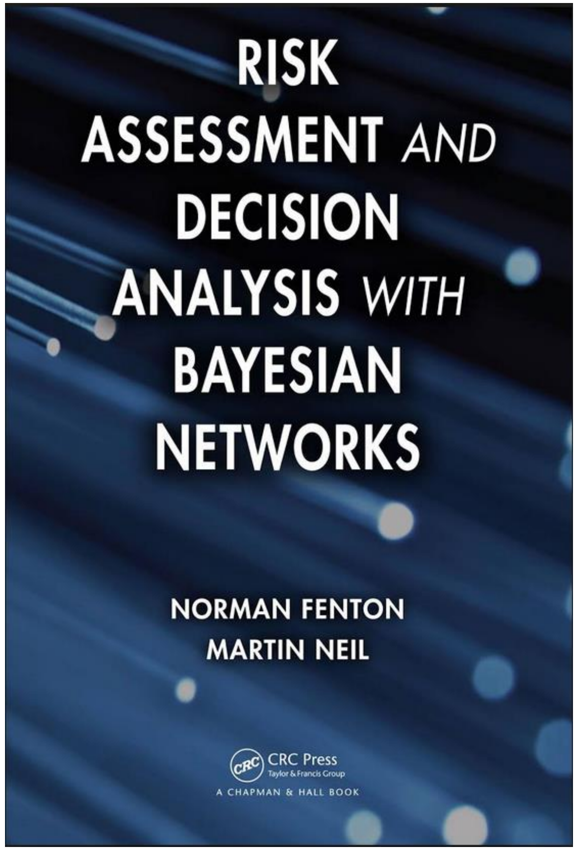
- Rolling back the contexts that were set for a specific Global Risk:

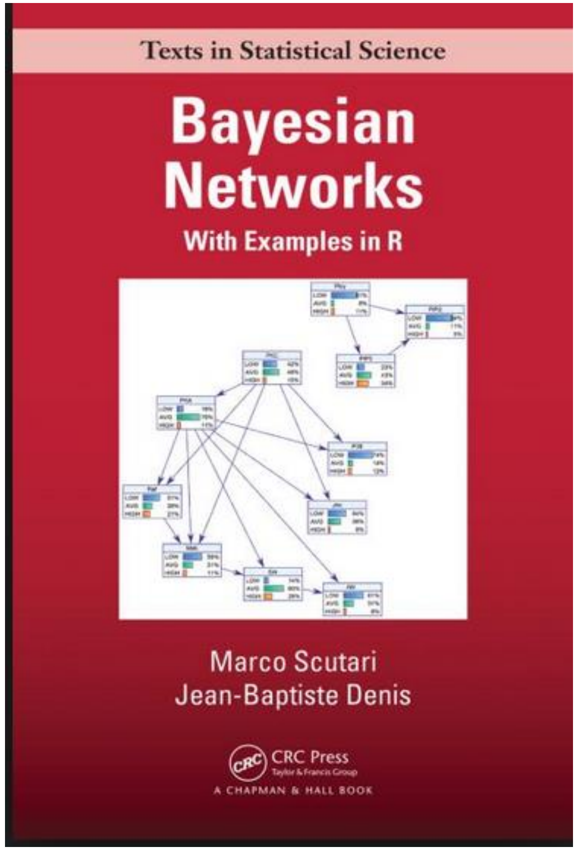
$$\begin{aligned} metaRule_3 \rightarrow & \textbf{ON} : ReceivedGlobalRisk(r) \wedge ReceivedContext(context_{data}) \\ & \textbf{IF} : context.level \leq T_{safe} \\ & \textbf{THEN} : REMOVE(GlobalRisk, r) \end{aligned}$$

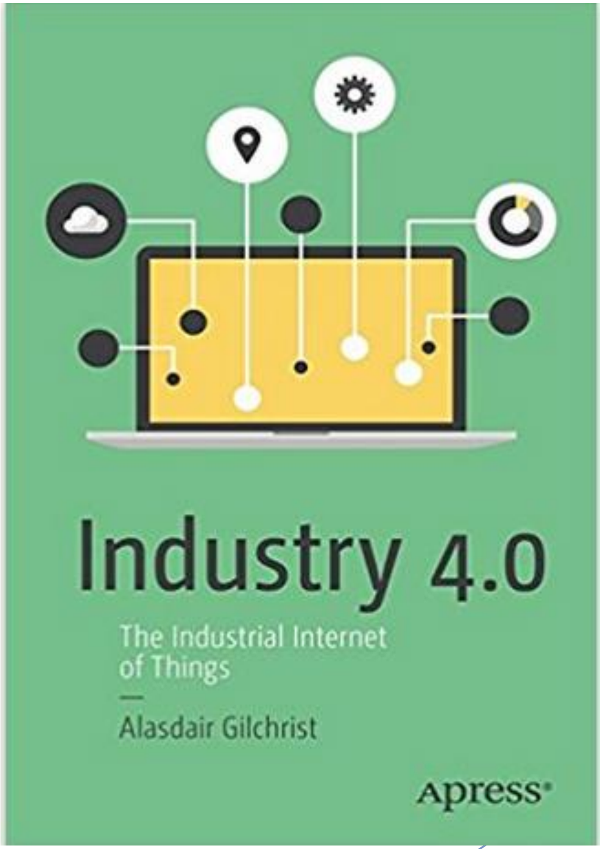
References

- Fenton, N., & Neil, M. (2012). *Risk assessment and decision analysis with Bayesian networks*. Crc Press.
- Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., ... & Scarfone, K. (2013). Guide to attribute based access control (ABAC) definition and considerations (draft). *NIST special publication*, *800*(162).
- Teimourikia, M., Fugini, M., & Raibulet, C. (2017, June). Run-Time Security and Safety Management in Adaptive Smart Work Environments. In *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2017 IEEE 26th International Conference on* (pp. 256-261). IEEE.
- Teimourikia, M., & Fugini, M. (2017). Ontology development for run-time safety management methodology in Smart Work Environments using ambient knowledge. *Future Generation Computer Systems*, *68*, 428-441.

Suggested Readings







Contacts

- To find the list of publications for more details:
  - https://scholar.google.it/citations?user=tH8DvigAAAAJ&hl=en
  - https://www.researchgate.net/profile/Mahsa_Teimourikia
  - http://home.deib.polimi.it/teimourikia/
- Feel free to contact me at:
  - Mahsa.teimourikia@polimi.it

Thank You!