Air Traffic Management Security Research in SESAR

J Hird (EUROCONTROL), M Hawley (Winsland Ltd), C Machin (AZTECH BVBA)

SecATM Workshop
ARES 2016
Salzburg, Austria
02/09/2016

Presenter : John Hird

EUROCONTROL

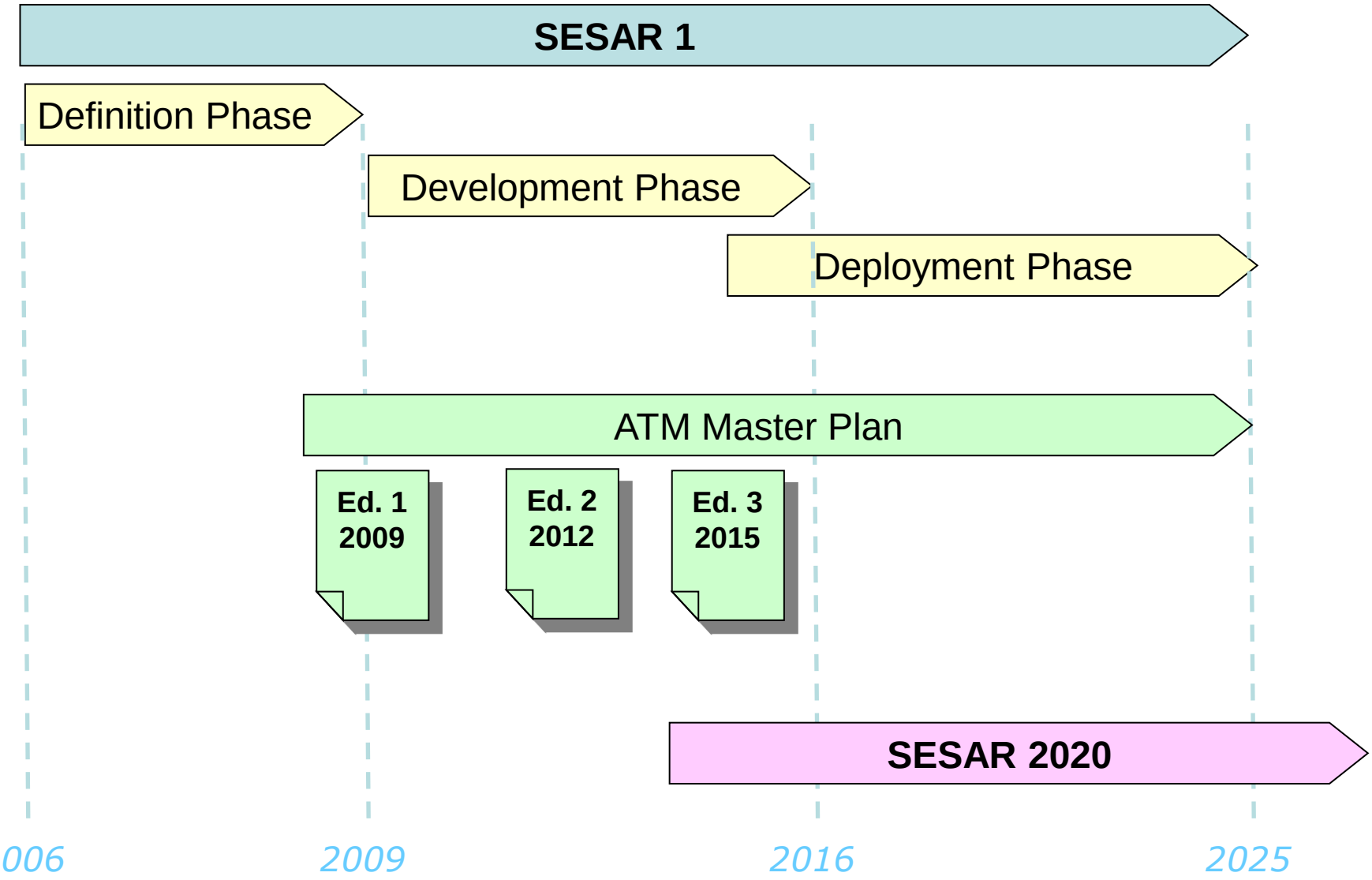
SESAR JOINT UNDERTAKING

Topics

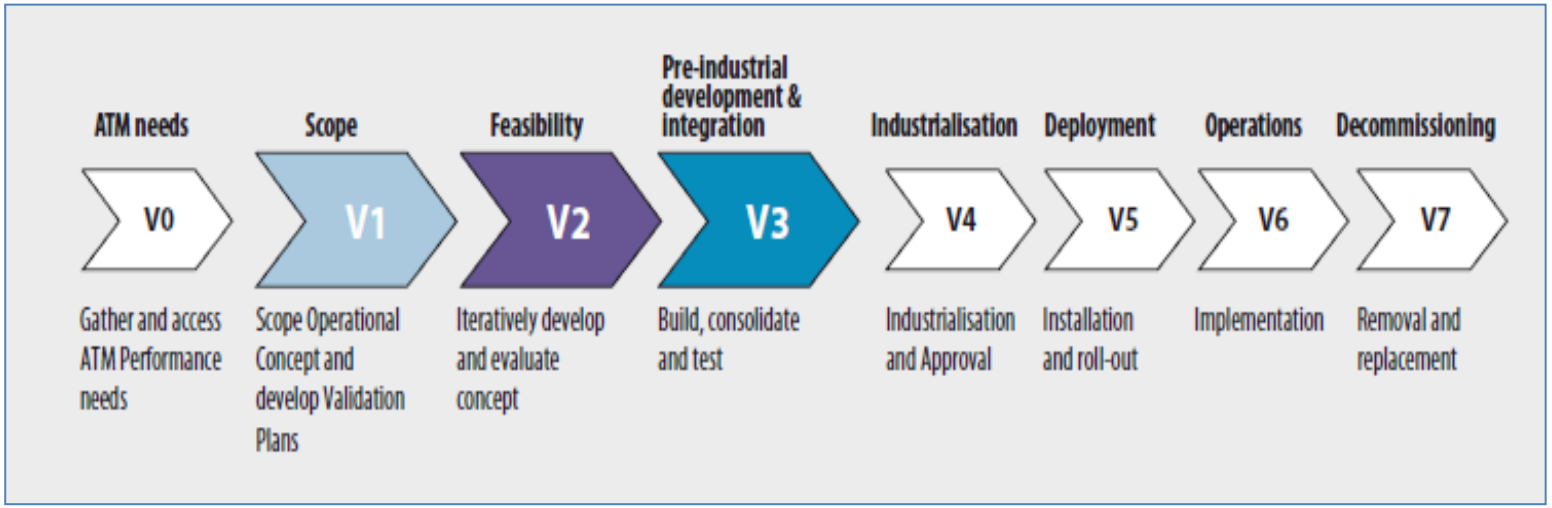
- SESAR Background
- The Scope of ATM Security
- The Evolving Risk Environment
- Myth Busting
- Security Risk Management
- Security Case
- Security Reference Material – Components
- Security Database Application
- Supporting the Projects
- Conclusions
- Questions

SESAR BACKGROUND

SESAR Programme Evolution



E-OCVM



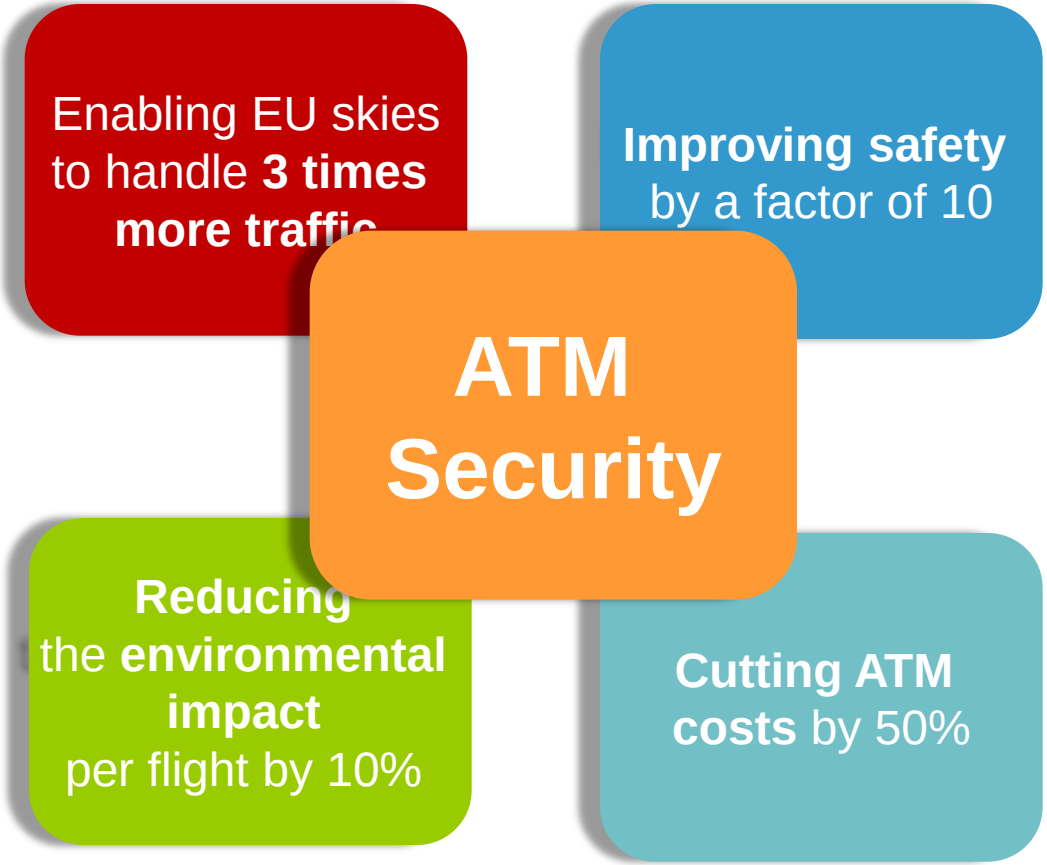
European Operational Concept Validation Methodology

SESAR focussed on :

- *V1 - Scope*
- *V2 - Feasibility*
- *V3 – Pre-industrial development & integration*

THE SCOPE OF ATM SECURITY

SESAR Key Performance Areas (KPAs)



Failing to adequately address security - impacts SESAR KPAs and other goals

ATM Security within Aviation Security

Airport Security

- Safeguarding of the airport

Aircraft Security

- Safeguarding of the aircraft

Airspace Security

- Safeguarding of the airspace

ATM Security

- **Safeguarding of the ATM System**
- **Collaborative support to national / Pan European aviation security incident management**

ATM System Assets – What Are We Trying to Protect?

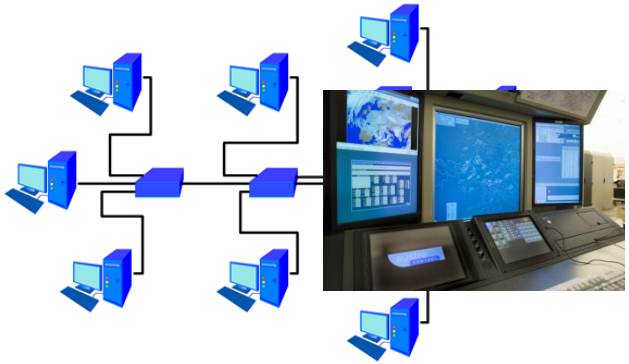
Service Provision

Physical: *e.g. Communications, Navigation, Surveillance (CNS), ATM centres, ...*

Staff: *Operational, Engineering, IT …*

Information: *Operational, Historical*

Organisational: *Financial, Reputation*



Information Systems

Staff

CNS Systems

ANSP Facilities

Service Provision

Potential Consequences of an Attack – Impact Areas

Personnel	Stress, minor injury, …, fatality
Capacity	Reduction, loss
Performance	Reduction, loss
Economic	Financial loss
Branding	Reputation
Regulatory	Breach of requirement
Environment	Impact on environment

EUROCONTROL

Threats past …

… and present!

Relationship between Safety and Security

We call **SAFETY** everything related to accidental events able to affect material and people (*failures,* …).

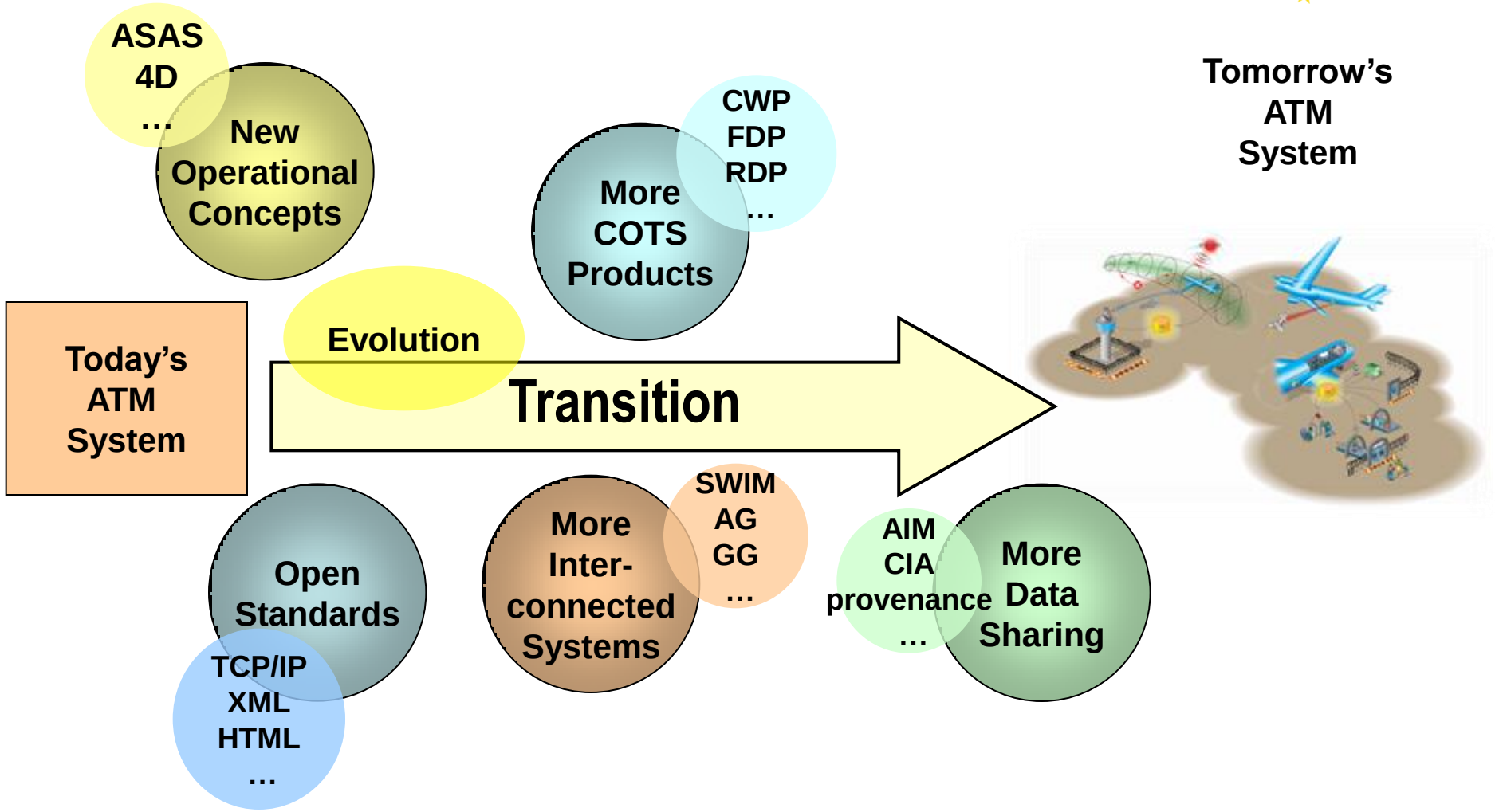
SECURITY concerns the prevention of deliberate malicious acts aimed at impacting the ATM system as a whole (*theft*, *hacking, jamming, spoofing, DoS*…).

Whatever can happen accidentally can be caused deliberately…
… the potential impact may be the same

12

THE EVOLVING RISK ENVIRONMENT

The Transition to the New System

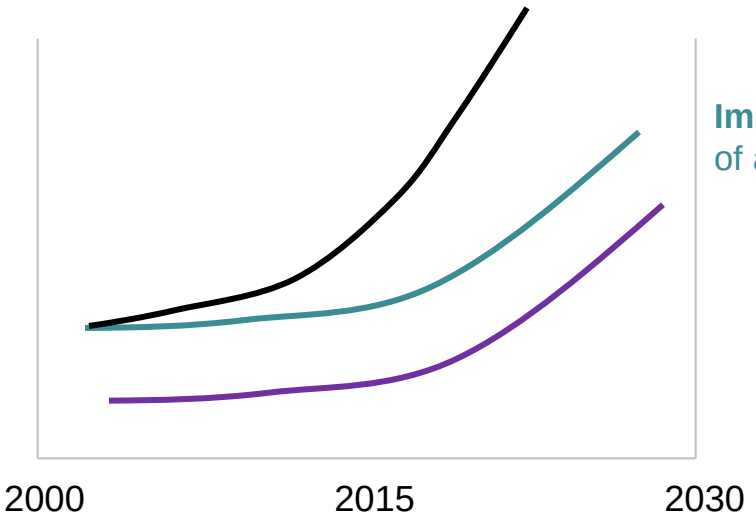


Risk Evolution in the Changing Security Environment

Risk = f (Impact, Likelihood)

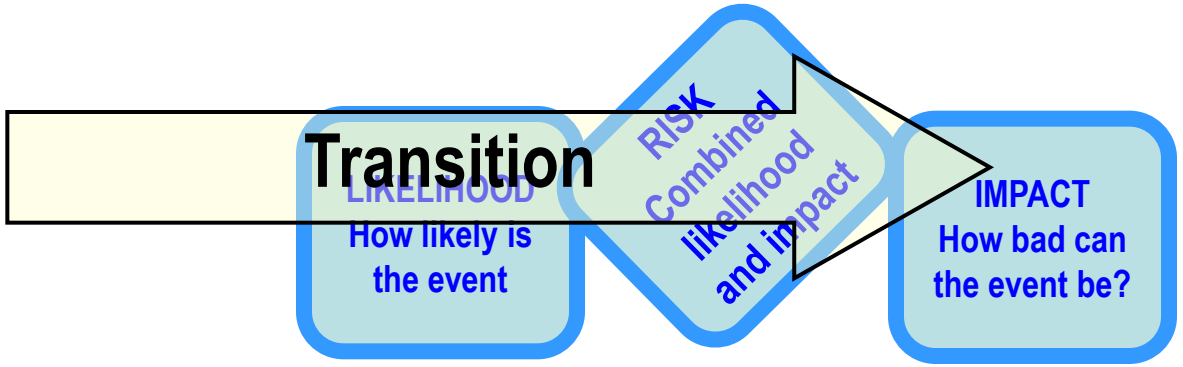
Drivers - increased hacking; criminality; State sponsorship

Likelihood (probability) of attack on ATM



Impact (severity) of attack on ATM

Drivers – system interdependency; data sharing



ATM Security Evolution

SESAR ATM Security Reference Material, 2016

SESAR 1

SESAR 2020

EC 2096/ 2005, CR

EC 1035/ 2011, CR

Dir 2016/ 1048, NIS

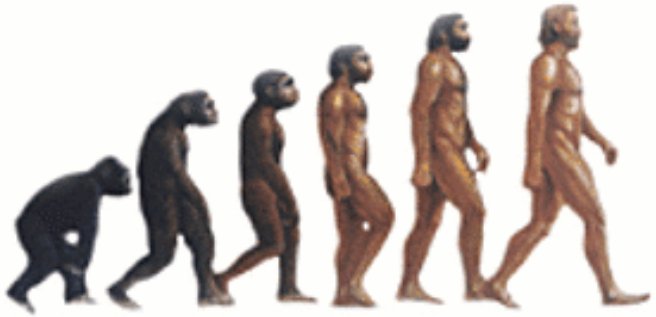
Doc 8973 AVSec

Doc 9854 ATM Op Concept, 2005

Annex 17 amend. 12, 2011 (ATSP, cyber)

Doc 9985 ATM Sec, 2013 (Secure design)

Doc 30 AVSec, Ed 13, 2010 (Ch 13, ATM Sec)



2001

2009

2016

MYTH BUSTING

ATM is not a Target?

Absence of evidence ≠ Absence of threat
Many compromises not discovered for years

Why Attack ATM or other Critical Infrastructures?

- To deny, degrade, disrupt, or destroy information systems and gain publicity

Potential players :

- Hackers/hacktivists – seeking challenge, notoriety, supporting ideological/political beliefs
- Terrorists – seeking a visible impact on a significant infrastructure
- Nation states –strategic target if state relationships deteriorate; possibility of military conflict

The target of the attack is not the system → it's the public's confidence in the integrity of networks and systems

Information sharing on ATM security incidents?

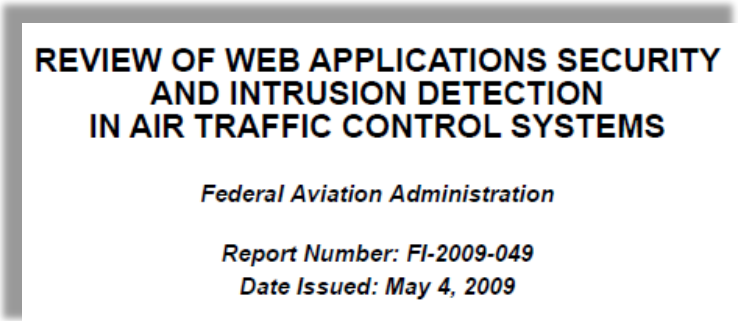
No legal requirement - Difficult to establish – Sensitive (commercially, reputationally)

ATM has never been attacked - ~~Imagine…..~~

- Theft of copper, batteries and other equipment ✓
- Injection of data, spoofing of systems ✓
- Unauthorised access to operational centers ✓
- Leaving 'suspect' packages to cause operational disruption ✓ ✓
- Electronic hacking into data systems ✓
- Deliberate use of substandard products in operational systems ✓
- IT systems containing unauthorised programmes (and viruses) ✓
- System overload (Denial of service attacks) ✓
- GPS jamming ✓

Luckily, so far :

- "Known" financial impact not substantial
- No businesses severely impacted
- No injuries or loss of life


REVIEW OF WEB APPLICATIONS SECURITY AND INTRUSION DETECTION IN AIR TRAFFIC CONTROL SYSTEMS

Federal Aviation Administration

Report Number: FI-2009-049
Date Issued: May 4, 2009

FAA ATM Systems

Confidentiality
Integrity
Availability

2006 :

- Web-based viral attack infected ATC systems I
- Part of ATC system in Alaska had to be shut down A

2008 :

- Hackers briefly controlled FAA critical network servers I

2009 :

- Hackers breached public-facing website I
- Gained unauthorized access to personal information on 48,000 current and former employees C

Audit revealed : 3800+ vulnerabilities in 70 Web apps (760 high-risk)

"In our opinion, unless effective action is taken quickly, it is likely to be a matter of when, not if, ATC systems encounter attacks that do serious harm to ATC operations"

REVIEW OF WEB APPLICATIONS SECURITY AND INTRUSION DETECTION IN AIR TRAFFIC CONTROL SYSTEMS

Federal Aviation Administration

Report Number: FI-2009-049
Date Issued: May 4, 2009

Security Incidents

Many recent aviation-related security incidents impact ATM, Airlines, and Aircraft. In addition, security incidents have occurred in other critical infrastructures.

Increasing levels of

- connectedness
- data sharing
- complexity
- use of COTS and standards

combined with

- lack of awareness
- questionable diligence

result in

- additional vulnerabilities

Security Incidents

ATM

25th April 2016

Open Season - As the aviation industry gets smarter, cybersecurity vulnerabilities threaten US airspace

http://www.airtrafficmanagement.net/2016/04/open-season/

6th October 2015

FAA Proposes $1.9 Million Civil Penalty Against SkyPan International for Allegedly Unauthorized Unmanned Aircraft Operations

https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19555

17th August 2015

Upgrade problem in FAA ERAM system causes outage - software complexity in critical infrastructures

http://thehill.com/policy/cybersecurity/251310-software-limits-exposed-in-air-traffic-outage

16th June 2015

Aircraft disappear from radar due to overload of Mode S transponders. This overload was caused by testing on the ground, where producers of radio navigation aids, radars and passive radio-locators were testing. Could be used as a threat.

http://ekonomika.idnes.cz/letadla-mizela-z-radaru-mohl-za-to-zrejme-test-ceskeho-vyrobce-p6l-/eko-doprava.aspx?c=A150616_160048_eko-doprava_wlk

27th May 2015

Belgium ATC outage caused by power surge. Not intentional, however, similar intentional act could have similar impact.

http://www.rtve.es/noticias/20150527/belgica-cierra-espacio-aereo-averia-centro-control-del-trafico-aereo/1151260.shtml

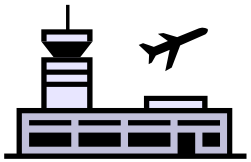
http://www.avweb.com/avwebflash/news/Power-Surge-Closes-Belgian-Airspace-224166-1.html

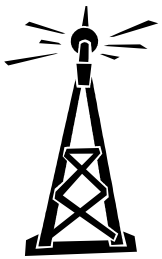
http://www.independent.co.uk/travel/news-and-advice/belgian-airspace-closed-air-traffic-control-failure-grounds-all-flights-causing-chaos-at-brussels-airport-10278525.html

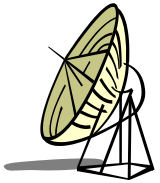
9th April 2015

CAA report on incident 19 Apr 2015

http://www.airproxboard.org.uk/docs/423/2015049.pdf







Security Incidents

Airlines

22nd March 2016

ANA Software Glitch Delays Thousands of Domestic Flights in Japan

http://www.aviationtoday.com/av/commercial/87475.html?hq_e=el&hq_m=3226739&hq_l=10&hq_v=a6829d2557

10th August 2015

Airlines under siege, lack of reporting requirement for hacking incidents

http://thehill.com/policy/cybersecurity/250614-airlines-under-siege-from-hackers

29th July 2015

United Airlines hacked by sophisticated hacking group

http://thehackernews.com/2015/07/united-airlines-hacked.html

21st June 2015

LOT airlines grounded by computer hack.

http://www.bbc.com/news/world-europe-33219276

Aircraft

17th April 2016

Drone hits British Airways Aircraft at Heathrow

http://www.bbc.com/news/uk-36067591

22nd February

Drones Pose Real Threat to Civil Aviation

http://www.bbc.com/news/business-35577124

19th February 2016 :

Serious Incident Between Drone And A320 at Paris Charles De Gaulle Airport

https://www.bea.aero/en/investigation-reports/notified-events/detail/event/quasi-collision-avec-un-drone-en-approche-1/

26th February 2016 :

Two more high-risk near misses between passenger aircraft and drones – at Heathrow and Manchester airports

http://www.theguardian.com/technology/2016/feb/26/drone-wingspan-away-jet-landing-heathrow

9th June 2015

Security Incidents

Other Critical Infrastructure

28th April 2016

German nuclear plant hit by computer viruses

http://www.bbc.com/news/technology-36158606

22nd April 2016

Smart city transport infrastructure easily hacked

http://go.reg.cx/seml/51445/57463c7f/69f80530/2kL2

18th April 2016

Weaknesses in mobile phone network interconnection systems (C7, CCSS7)

https://www.theguardian.com/technology/2016/apr/18/phone-number-hacker-read-texts-listen-calls-track-you?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+main+NEW+H&utm_term=167804&subid=9878997&CMP=EMCNEWEML6619I2

5th October 2015

Cybersecurity risks to civil nuclear infrastructure grow. https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks

Report -
https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf

24th March 2016

Bug pops secure doors at airports, hospitals

http://www.theregister.co.uk/2016/04/04/devastating_bug_pops_secure_doors_at_airports_hospitals

24th March 2016

Water treatment plant hacked, chemical mix changed for tap supplies

http://go.reg.cx/seml/51445/5721527f/88df761e/2knf

26th February 2016 :

Hackers behind Ukraine Power Cuts

http://www.bbc.com/news/technology-35667989

29th July 2013

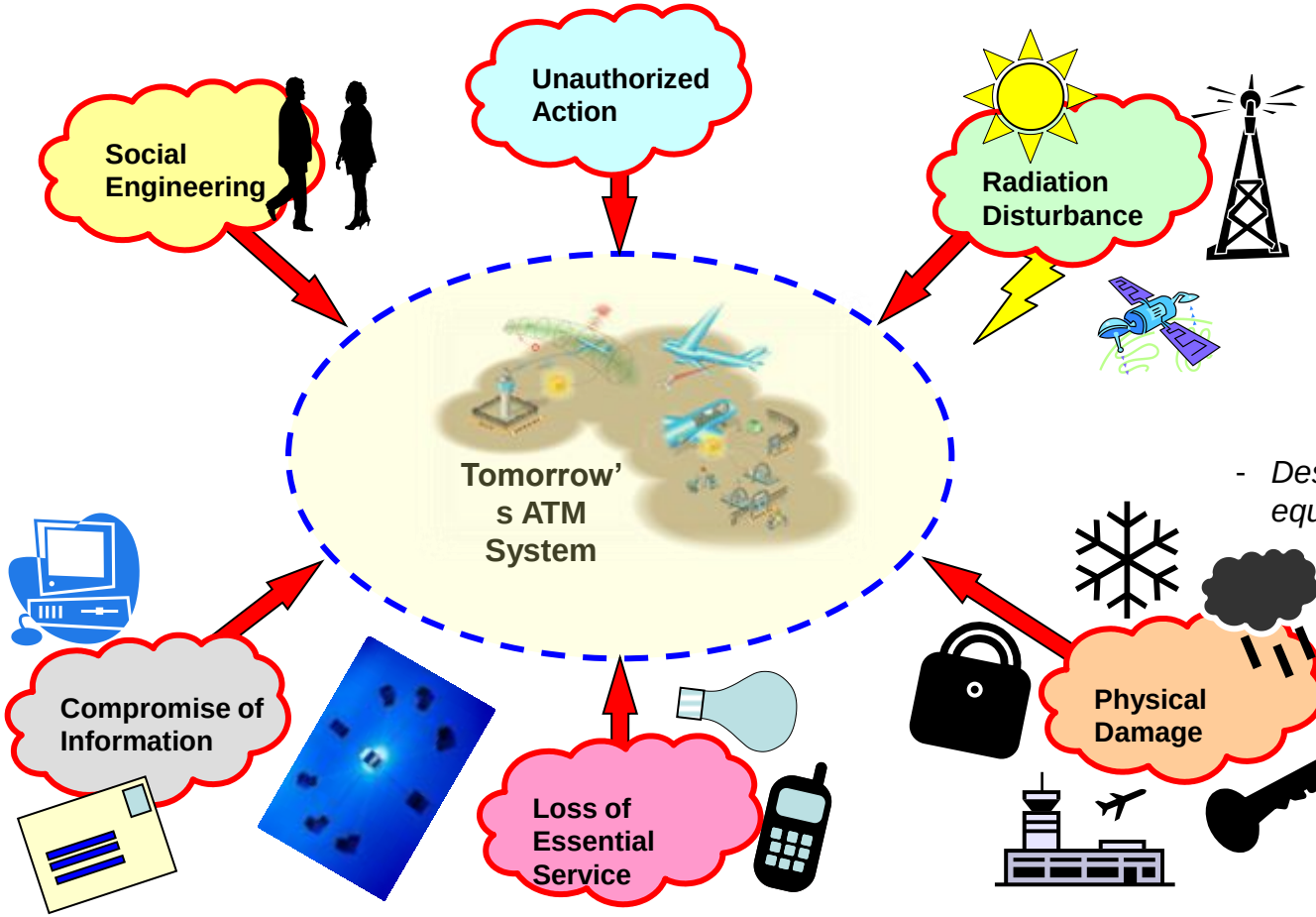
Successful GPS spoofing of yacht at sea

http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea

Potential Threats

- *Corruption of data*
- *Unauthorised use of equipment*

- *Electromagnetic radiation/pulses*



- *Destruction of equipment or media*

- *Tampering with HW/SW*
- *Eavesdropping*
- *Theft of media, documents, equipment*

- *Communications*
- *Power*

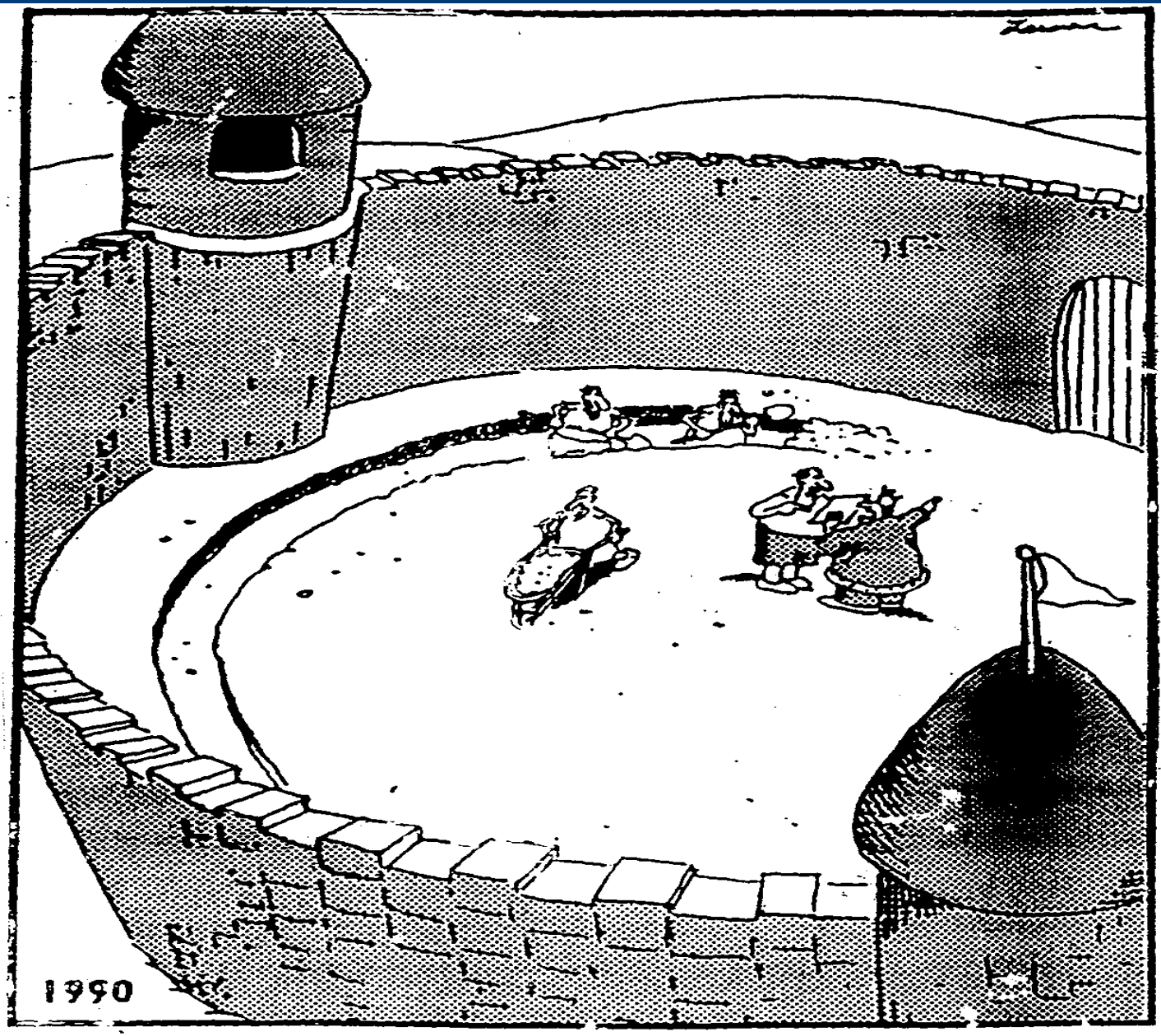
"The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning."

- Charles Tremper

SECURITY RISK MANAGEMENT

EUROCONTROL

How should you spend your money to gain a proportionate reduction in risk?



Suddenly, a heated exchange took place between the king and the moat contractor.

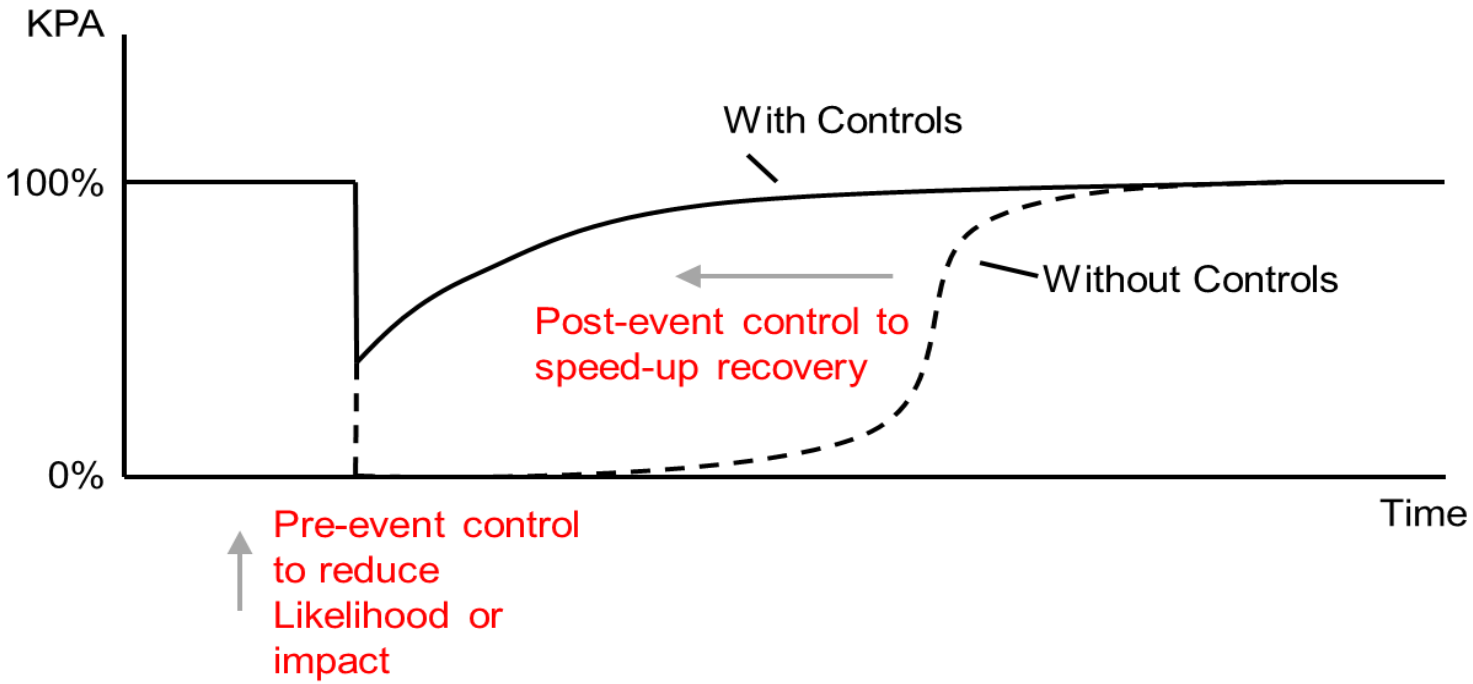
Security Risk Management – Goals

- *Prevent* an attack from being successful
- Implement an effective *response* to a successful attack
- *Recover* operational services to their pre-incident level as quickly as possible

"I think we need to take another look at your risk-management strategy."

Incident Preparedness and Operational Continuity Management **(IPOCM)**

- Preventing an incident by protecting the system from an attack
- Recovering to normal operations as safely/quickly as possible



- IPOCM is realised by performing a ***Security Risk Assessment*** to identify *what* needs to be protected and *how* to protect it

Security Risk Management - Means

Perform a security risk assessment

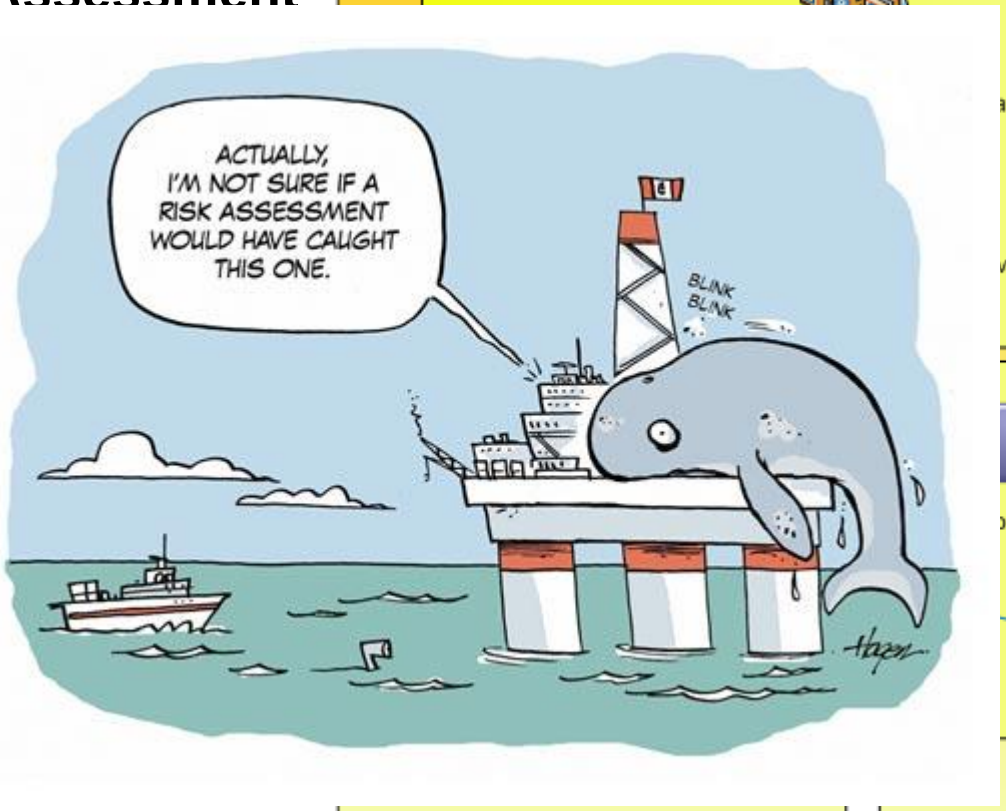
- Identify and evaluate risks
- Prioritize them
- Decide how to address (Treat, Transfer, Terminate, Tolerate)
- Reduce the risk of an attack by implementing a set of Controls (mitigation means) to :
  - Reduce the likelihood of the attack
  - Limit the impact of a successful attack

EUROCONTROL

The Security Risk Assessment Methodology

Identify :

- Assets
- Impacts on CIA
- Risks
- Controls



Security Risk Management Approach

- Address security *at all stages of the life-cycle*

  From concept development through to decommissioning

- *Design-in security* from the beginning

  Retrofitting can be expensive, time-consuming, not feasible

- Apply a *holistic approach* to security

  Assets to protect include people, information, infrastructure, …

- Apply a *common or harmonized approach*

  Enable the sharing, comparing, and aggregation of results

- Establish a *common, minimum level of security* across system

  Potential adversaries will exploit the weakest link

Risk Matrix

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

LIKELIHOOD
How likely is the event

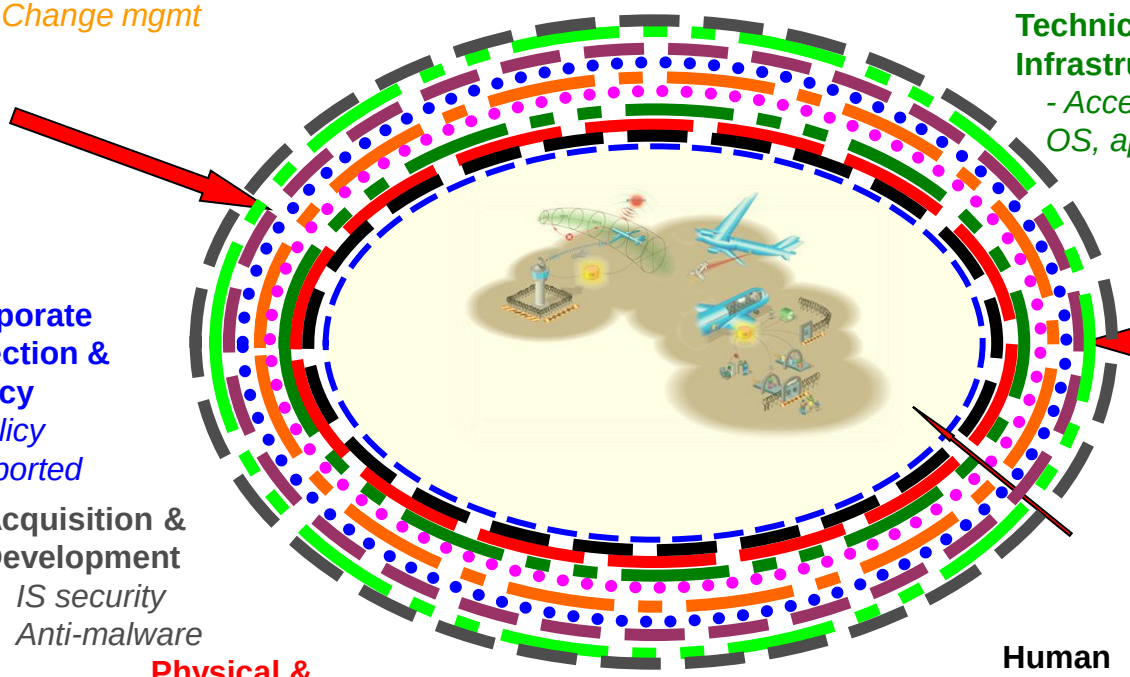
RISK
Combined likelihood and impact

IMPACT
How bad can the event be?

Holistic Approach to Controls

Operation of ICT Systems
- *Systems isolated*
- *Network security*
- *Backups*
- *Change mgmt*

Organisation, Culture & Management
- *Clear roles & Responsibilities*
- *Risks managed*



Technical Mechanisms & Infrastructure
- *Access control – networks, OS, applications, user mgmt.*

Compliance
- *Legal, Policy, Standards*

Corporate Direction & Policy
- *Policy supported*

Acquisition & Development
- *IS security*
- *Anti-malware*
- *…*

Physical & Environmental Security
- *Secure*

Monitoring & Audit
- *Logging*
- *Audits*

Human Resources
- *Training*
- *Vetting*

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology. Bruce Schneier

Risk Reduction – Control Examples

Controls to Reduce Impact :

- Network isolation
- Staff training
- Governance structure
- Redundancy, backups

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

Controls to Reduce Likelihood :

- Network isolation
- Physical protection
- Security staff

	Reviewed Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Low	Medium	High
1	Low	Low	Low	Medium	Medium

SECURITY CASE

Security Case

Security Case - an argument comprised of a number of claims

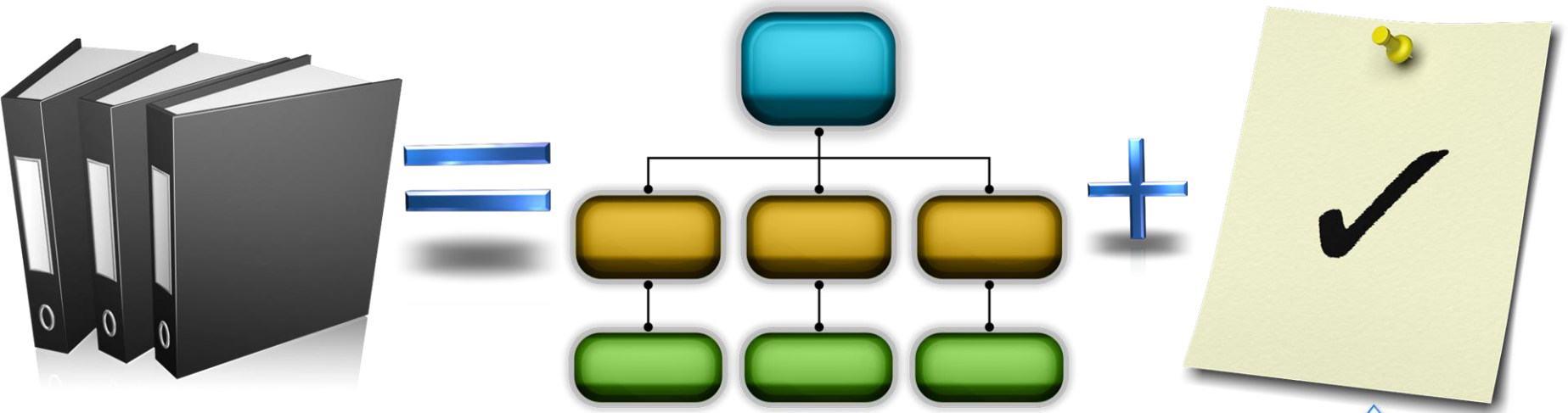
- A top-level claim (that the SESAR Solution is secure) is decomposed into a number of sub-claims
- If all sub-claims are demonstrated to be true, the top-level claim is true
- Claims are proven by collecting evidence
- The process of gathering evidence is called *assurance*

Ensuring that the Security Case is Trustworthy

- Standards and Best Practices are applied to develop and validate the requirements
- Experienced security experts are involved
- Operational and technical experts from the Solution are involved
- Peer review is carried out
- Evidence is approved by the Project Manager
- All regulatory requirements are met

Security Case

Security Case | Argument | Evidence



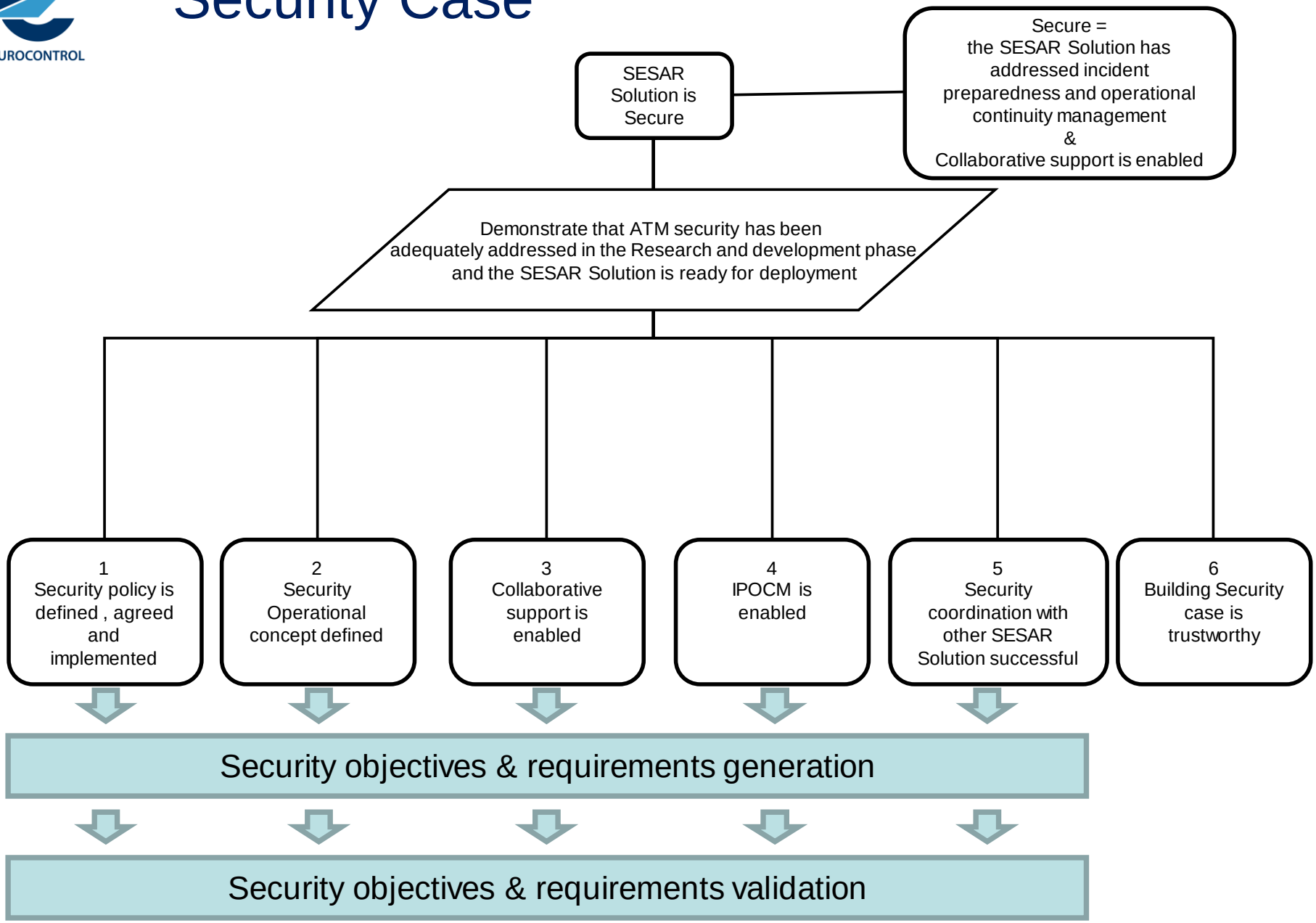
Driving the processes

Producing

Security Risk Assessment

& Assurance Activities

Security Case



SECURITY REFERENCE MATERIAL – COMPONENTS

Reference Material Components

SESAR JOINT UNDERTAKING

SESAR ATM Security Reference Material - Level 1

Document information	
Project Title	Security Support and Coordination Function
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	SESAR ATM Security R
Deliverable ID	D103
Edition	00.02.01
Template Version	03.00.00
Task contributors	
EUROCONTROL, ENAIRE, AIRBUS, DFS, ENA FINMECCANICA, and THALES	

Please complete the advanced properties of the document

Abstract

This document presents the SESAR ATM Security level **guidance on the security activities req industrialisation and deployment phases.**

This Level 1 version addresses immediate needs of techniques to deliver Evidence necessary for an AT

SESAR JOINT UNDERTAKING

SESAR ATM Security Reference Material - Level 2

Document information	
Project Title	Security Support and Coordination Function
Project Number	16.06.02
	EUROCONTROL
	SESAR ATM Security Reference Material
	D103
	00.02.01
	03.00.00

S, ENAV, EUROCONTROL, FREQUENT THALES

d properties of the document

ts the SESAR ATM Security Reference M ecurity activities required to move S eployment phases.

dresses immediate needs of Projects to use c idence necessary for an ATM Security Case.

SESAR JOINT UNDERTAKING

Minimum Set of Security Controls

Document information	
Project Title	Harmonised ATM Security best practices
Project Number	16.06.02
Project Manager	ENAV

f Security Controls

A, SELEX, THALES

mum set of security controls that each ATM uld adopt in order to reach a common minimum

nd information.

SESAR JOINT UNDERTAKING

SESAR ATM Security Model

Document information	
Project Title	SESAR ATM Security Model
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	SESAR ATM Security Model
Deliverable ID	D133
Edition	00.01.00
Template Version	03.00.00
Task contributors	
SELEX (L), AENA, FREQUENTIS, INDRA, EUROCONTROL, AIRBUS	

Please complete the advanced properties of the document

Abstract

This document provides the reader with information on the development of a 'Security Model', which is used to assess the security of CFAs/SESAR Solutions. The document covers the genesis of the Security Model that took place under WP16.02.02 and the further development of requirements prior to implementation as an MS Access database.

SESAR JOINT UNDERTAKING

Completed Security Database Application

Document information	
Project Title	Security Support and Coordination Function
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	Completed Security Database Application
Deliverable ID	D131
Edition	00.01.00
Template Version	03.00.00
Task contributors	
EUROCONTROL	

Please complete the advanced properties of the document

Abstract

This document serves as a user manual for the security database application CTRL_S.

Level 1

SESAR JOINT UNDERTAKING

SESAR ATM Security Reference Material - Level 1

Document information	
Project Title	Security Support and Coordination Function
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	SESAR ATM Security Reference Material - Level 1
Deliverable ID	D103
Edition	00.02.01
Template Version	03.00.00
Task contributors	
EUROCONTROL, ENAIRE, AIRBUS, DFS, ENAV, FREQUENTIS, INDRA, NAV PORTUGAL, FINMECCANICA, and THALES	

Please complete the advanced properties of the document

Abstract

This document presents the SESAR ATM Security Reference Material – Level 1. It provides high-level **guidance on the security activities required to move SESAR Solutions onto the industrialisation and deployment phases.**

This Level 1 version addresses immediate needs of Projects to use common methods, tools and techniques to deliver Evidence necessary for an ATM Security Case.

ATM Security Reference Material - Level 1

High-level guidance on the conduct of security management and associated assurance activities to enable SESAR Solutions to be validated to V3.

Topics addressed include :

- *Security Policy;*
- *Security Objectives;*
- *Security Risk Management;*
- *Relationship between Security and Safety*
- *Security Risk Assessment*
- *Security Case*

Annex 1 : Frequently Asked Questions

Level 2

SESAR JOINT UNDERTAKING

SESAR ATM Security Reference Material - Level 2

Document information	
Project Title	Security Support and Coordination Function
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	SESAR ATM Security Reference Material - Level 2
Deliverable ID	D103
Edition	00.02.01
Template Version	03.00.00
Task contributors	
AENA, AIRBUS, DFS, ENAV, EUROCONTROL, FREQUENTIS, INDRA, NAV Portugal, FINMECCANICA, and THALES	

Please complete the advanced properties of the document

Abstract

This document presents the SESAR ATM Security Reference Material – Level 2. It provides **guidance on the security activities required to move SESAR Solutions onto the industrialisation and deployment phases.**

This Level 2 version addresses immediate needs of Projects to use common methods, tools and techniques to deliver Evidence necessary for an ATM Security Case.

ATM Security Reference Material - Level 2

Detailed, practical guidance on how to conduct security management activities. Topics addressed include :

- *Security risk assessment*
  - *asset identification*
  - *threat scenarios*
  - *Impact, likelihood, risk evaluation*
- *Risk treatment*
- *…*

Annex 1 : Threat catalogue

Annex II : Handling of sensitive information

Annex III : RPAS

Annex Iv : Cost-effectiveness of design-in security

Annex V : Alignment of ATM Security & EATMA

MSSCs

SESAR JOINT UNDERTAKING

Minimum Set of Security Controls

Document information	
Project Title	Harmonised ATM Security best practices
Project Number	16.06.02
Project Manager	ENAV
Deliverable Name	Minimum Set of Security Controls
Deliverable ID	D137
Edition	00.01.00
Template Version	03.00.00
Task contributors	
AIRBUS, ENAV, EUROCONTROL, INDRA, SELEX, THALES	

Abstract

This document specifies the minimum set of security controls that each ATM organization, project or solution should adopt in order to reach a common minimum baseline of ATM security.

The controls apply to ATM services and information.

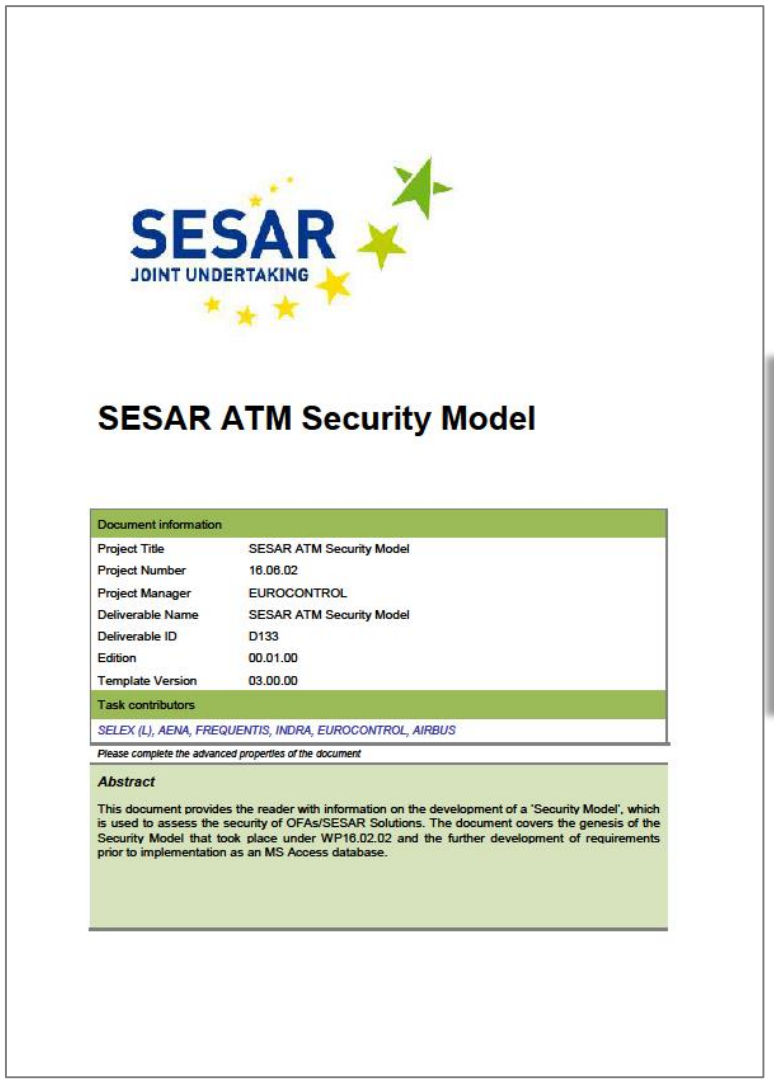
Minimum Set of Security Controls

This specifies a minimum set of security countermeasures that all SESAR Solutions should apply.

Document structure based on ISO 27002:2013 security control clauses e.g.

- Security Policy
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Physical and Environmental Security
- Operations Security
- Communications Security
- …

Security Model



SESAR ATM Security Model

Document information	
Project Title	SESAR ATM Security Model
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	SESAR ATM Security Model
Deliverable ID	D133
Edition	00.01.00
Template Version	03.00.00
Task contributors	
SELEX (L), AENA, FREQUENTIS, INDRA, EUROCONTROL, AIRBUS	

Please complete the advanced properties of the document

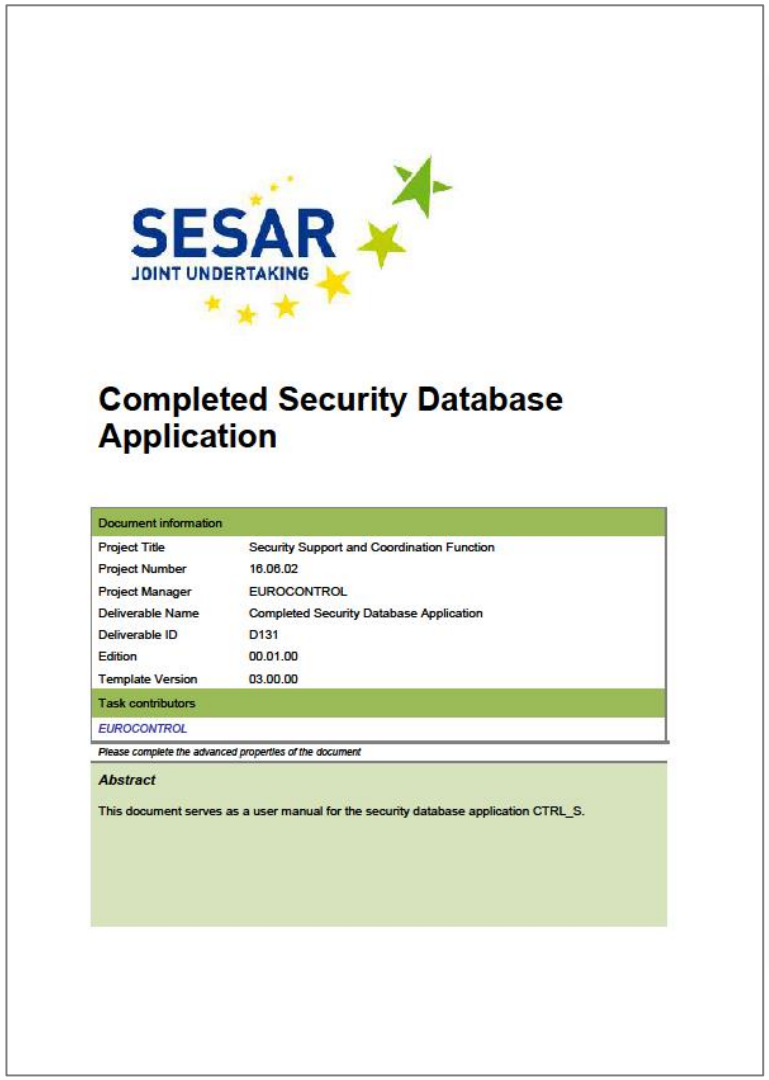
Abstract

This document provides the reader with information on the development of a 'Security Model', which is used to assess the security of OFAs/SESAR Solutions. The document covers the genesis of the Security Model that took place under WP16.02.02 and the further development of requirements prior to implementation as an MS Access database.

ATM Security Model

This describes the development history of the database model which underlies the security database application (CTRL_S).

Security Database Application (CTRL_S)



SESAR JOINT UNDERTAKING

Completed Security Database Application

Document information	
Project Title	Security Support and Coordination Function
Project Number	16.06.02
Project Manager	EUROCONTROL
Deliverable Name	Completed Security Database Application
Deliverable ID	D131
Edition	00.01.00
Template Version	03.00.00
Task contributors	
EUROCONTROL	

Please complete the advanced properties of the document

Abstract

This document serves as a user manual for the security database application CTRL_S.

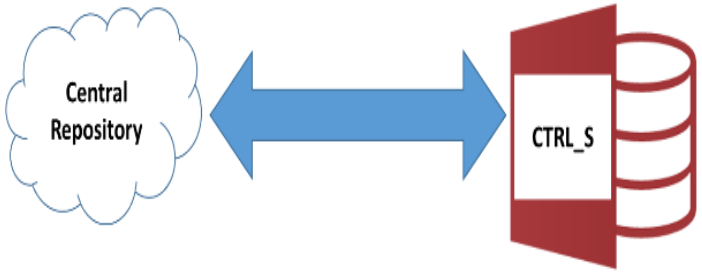
Security Database Application – CTRL_S)

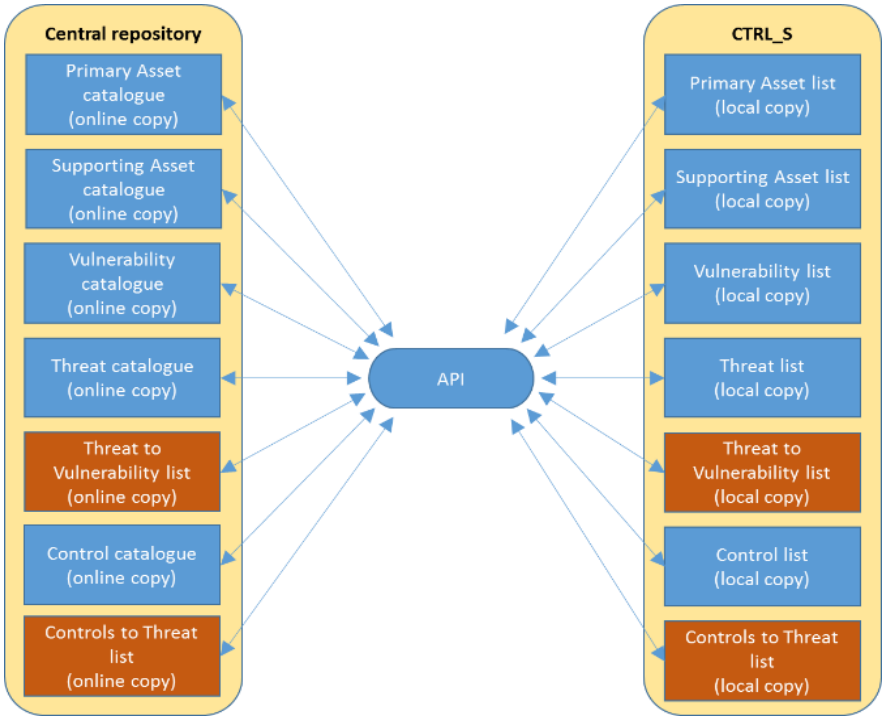
- Using a forms-based interface, this application guides the user through the workflow required to perform a security risk assessment.
- The asset, threat, and control catalogues are incorporated to support the process.
- Risk assessment results from different solutions may be uploaded to a centralised database and aggregated, allowing a high-level view of the security posture of the overall system to be obtained.

SECURITY DATABASE APPLICATION (CTRL_S)

Security Database Application

- Forms-based database application
- Captures the SESAR SecRAM process
- Supports collaborative approach
- Supports cross-sectional analysis of multiple risk assessments





CTRL_S – Menu Screen

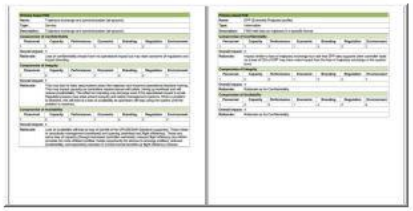
- abc

CTRL_S – Export screen

Menu | Assessment Detail Report | Export Menu

Security Assessment Summary Report Export

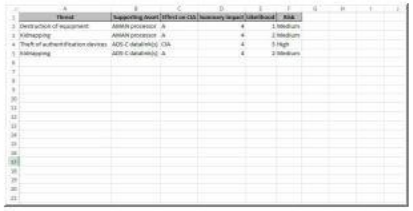
Export PA to Template Format PDF



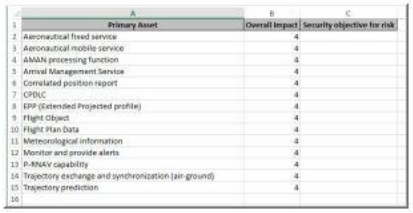
Export textual short overview RTF

Export PA short overview Excel

Export TH scenario overview Excel

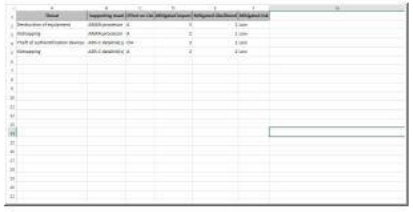


Export PA overall impact Excel



	Primary Asset	Overall Impact	Security objective for risk
2	Aeronautical fixed service	4	
3	Aeronautical mobile service	4	
4	AMAN processing function	4	
5	Arrival Management Service	4	
6	Correlated position report	4	
7	CPDLC	4	
8	EPP (Extended Projected profile)	4	
9	Flight Object	4	
10	Flight Plan Data	4	
11	Meteorological information	4	
12	Monitor and provide alerts	4	
13	P-RNAV capability	4	
14	Trajectory exchange and synchronization (air-ground)	4	
15	Trajectory prediction	4	
16			

Export TH mitigated scenario overview Excel

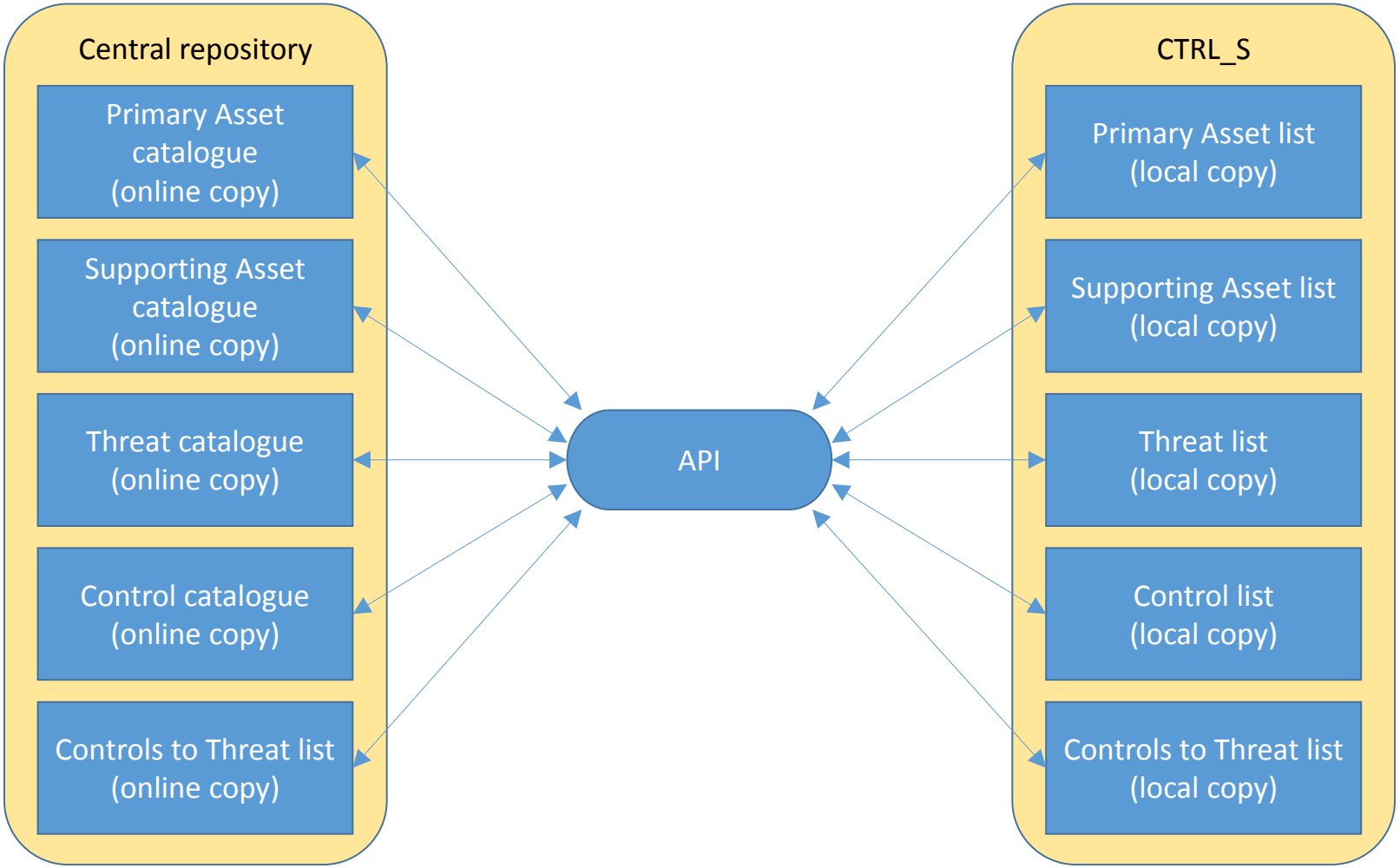


Export SA short overview Excel

Export all data to single Excel

Close

CTRL_S – Local App, Central Repository

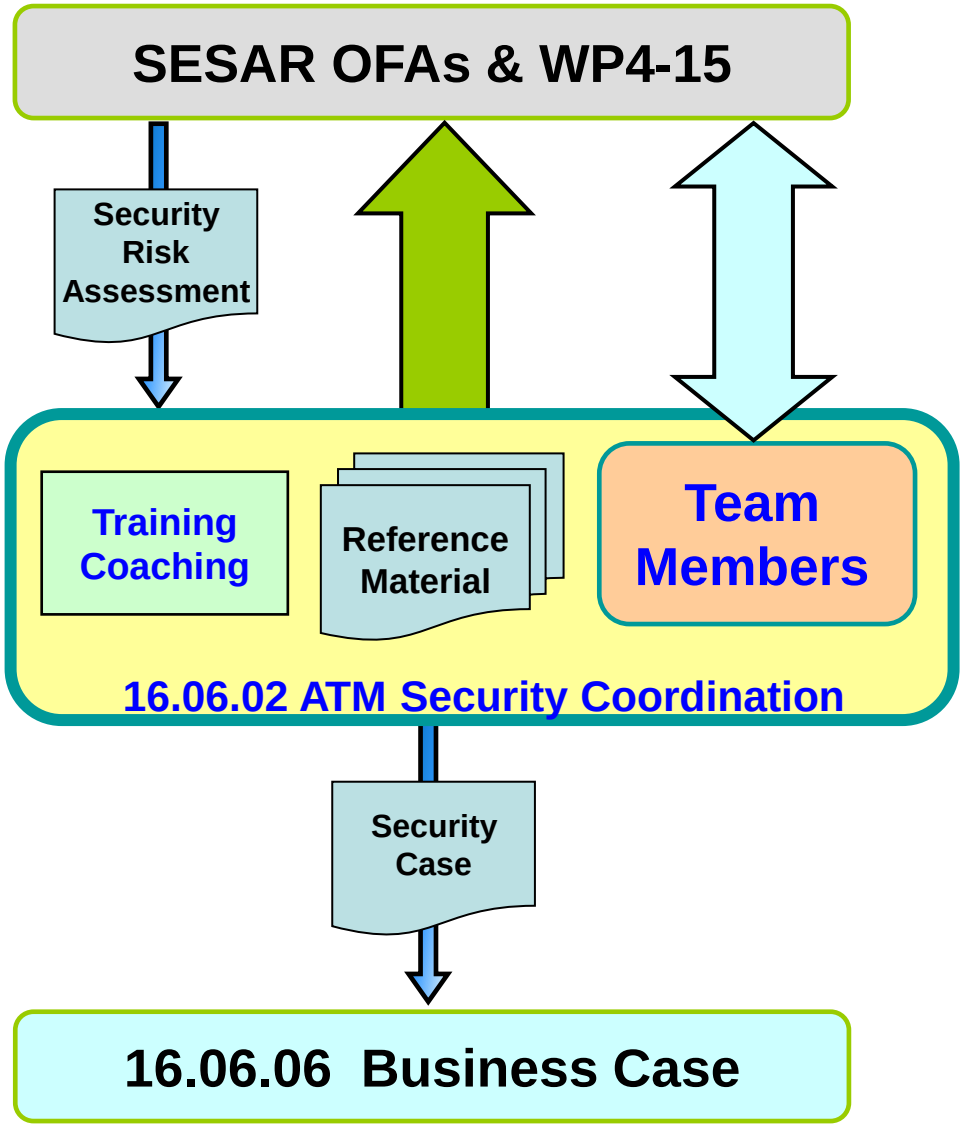


SUPPORTING THE PROJECTS

Project Interactions

- Awareness Material –
  - Explains the need for security
- Reference Material
  - What to do and how
- Coaching & Training

  Providing support in :
  - Applying the Reference Material
  - Performing Security Risk Assessments



Completed Risk Assessments

Risk Assessments Performed in Operational Focus Areas
System-Wide Information Management (SWIM)
Trajectory Management Framework and System Interoperability with air and ground data sharing
Low Visibility Procedures (LVPs) using Ground-Based Augmentation System (GBAS)
Airport safety nets
Enhanced Runway Throughput
Business and Mission Trajectory
Ground Based Separation Provision in En Route
Ground Based Separation Provision in the TMA
Enhanced Ground Based Safety Nets
Enhanced Arrival & Departure Management in Terminal Manoeuvring Area (TMA) and En Route
Integrated Surface Management
Airport Operations Management
Enhanced ATFCM processes
Network Operations Planning
Continuous Descent Operation
Controller Working Position (CWP) En Route and TMA
Remote Tower
Trajectory Management Framework
Initial 4-D Flight Path Control (i4D) and Controlled Time of Arrival (CTA)
Collaborative Network Operations Portal
Continuous Descent Operations

CONCLUSIONS

Achievements

SESAR has developed a comprehensive set of deliverables for ATM Security :

- *Awareness Material*
- *A Security Risk Assessment Methodology and supporting Guidance Material*
- *An approach to the development of a Security Case*
- *A Database Application which facilitates the recording, analysis and reporting of risk assessment results*

Support Activities

- *Awareness training, coaching and support provided to SESAR projects*
- *Risk assessments have been developed using the guidance material and tools*
- *Participation in system engineering reviews and security testing*
- *Support provided to development of SESAR Business Case*

Recommendations

- Security should be addressed throughout the development life-cycle and *designed-in* from the beginning
- Apply a *holistic approach* to security (addressing personnel, procedures, physical infrastructure and ICT)
- Apply *common or compatible* methods, tools and guidance material to permit the sharing, comparing and aggregation of results
- Establish a *common, minimum level of security* across the ATM system

EUROCONTROL

SESAR JOINT UNDERTAKING

Selling umbrellas in the sunshine?


Thank you!