How To SWIM Securely?

Patrizia Montefusco

09/11/2017, Krakow

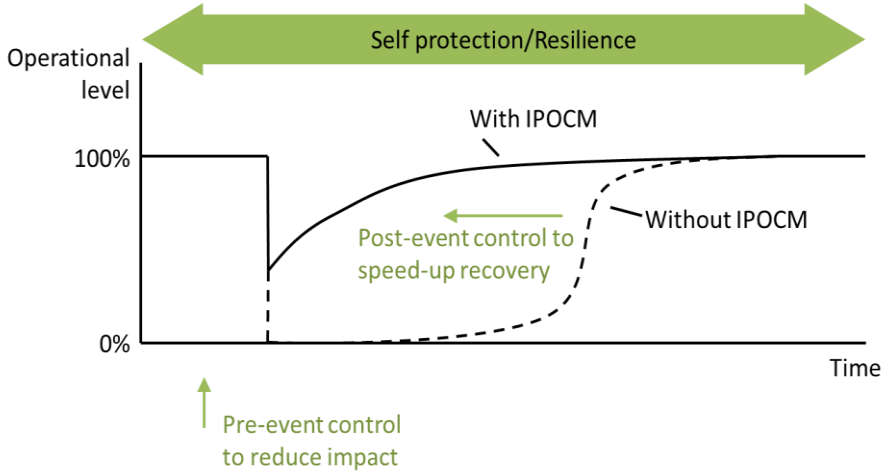
LEONARDO
SECURITY & INFORMATION SYSTEMS

Secure by Design : not only prevention…

From ICAO Doc 9854:

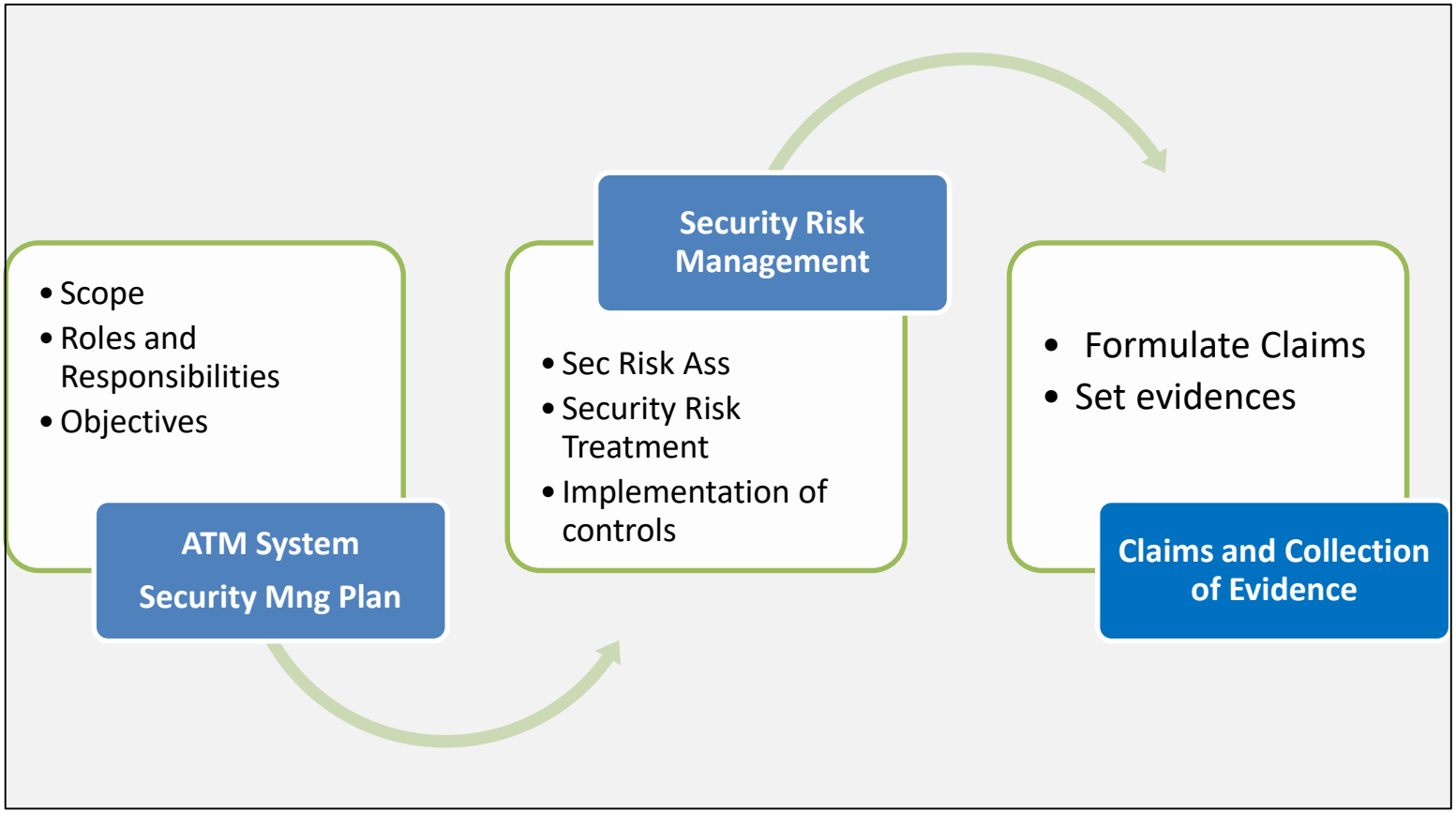
Security refers to the protection against threats that stem from intentional acts (e.g. terrorism) or unintentional acts (e.g. human error, natural disaster) affecting aircraft, people or installations on the ground. Adequate security is a major expectation of the ATM community and of citizens.
The ATM system should therefore contribute to security, and the ATM system, as well as ATM-related information, should be protected against security threats. Security risk management should balance the needs of the members of the ATM community that require access to the system, with the need to protect the ATM system.

A key aspect of ATM security is therefore ensuring that the ATM System is also prepared for the after-effects of an attack as well as preventing it in the first place.



SESAR 1-16.6.2 REFERENCE MATERIAL

Secure by Design : Information Security Assurance is an internal, non negotiable preliminary requirement in any modern ATM or ATM-related Technological component



Eurocae ED 205 Approach

How to Secure ATM information systems?

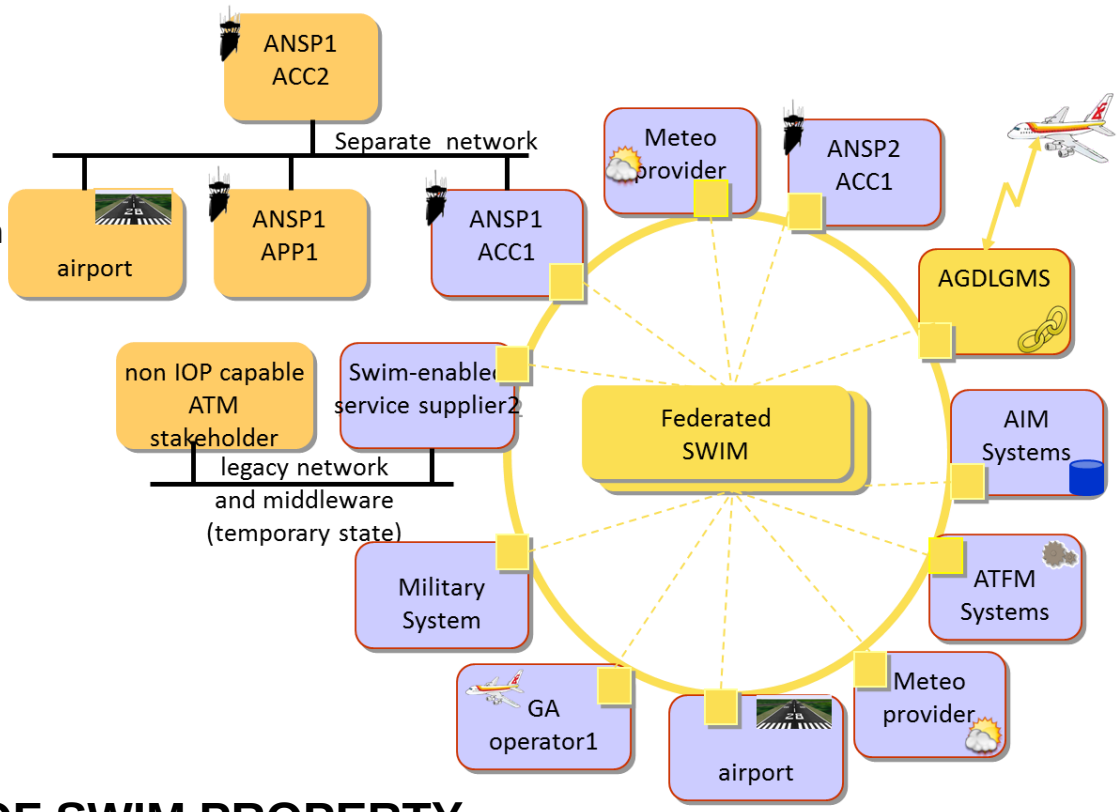
Leonardo believes that:

- An adequate maturity capability model based on commonly agreed metrics should be put in place for assurance purpose;
- International standards and commonly agreed best practices should be generally applied, in order to ensure uniformity of outputs and a fair, sustainable and cost-effective application, independently on customer, manufacturer or State in which the systems will work;
- Eurocae ED-205 is a good term of reference

FUTURE ATM SYSTEM INTERCONNECTION

The System of Systems nature of European ATM Network implies a large number of stakeholders requesting sharing of information

- A number of stakeholder\systems connected together thanks to a kind of “access point”.
- The set of «SWIM Nodes» realize the ring in the picture (i.e. so called SWIM Network – Network not in the sense of physical IP net)
- Many possible implementations of SWIM Node are possible. The «constraint» is that they need to be interoperable (i.e. expose agreed/standard interfaces/technologies)
- ATM Systems should introduce Authorized, Authenticated and Accountable (AAA) data

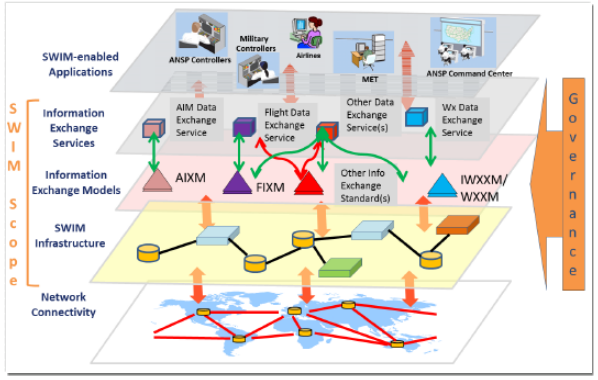


SECURITY HAS TO BE ONE OF SWIM PROPERTY

SESAR 1 SWIM
Concept Documents

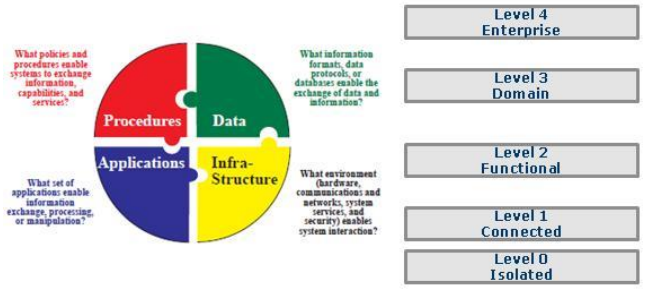
SWIM in a nutshell

- (SWIM Definition) *SWIM consists of standards, infrastructure and governance enabling the management of ATM information and its exchange between qualified parties via interoperable services.*

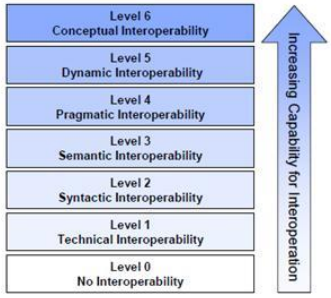


Ref. ICAO Doc 10039

- Information Systems Interoperability, especially in the ATM context, is a complex topic that may be faced from different perspectives: systems, data and governance.
  - SWIM covers mainly the syntactical, the semantic and technical interoperability layers.



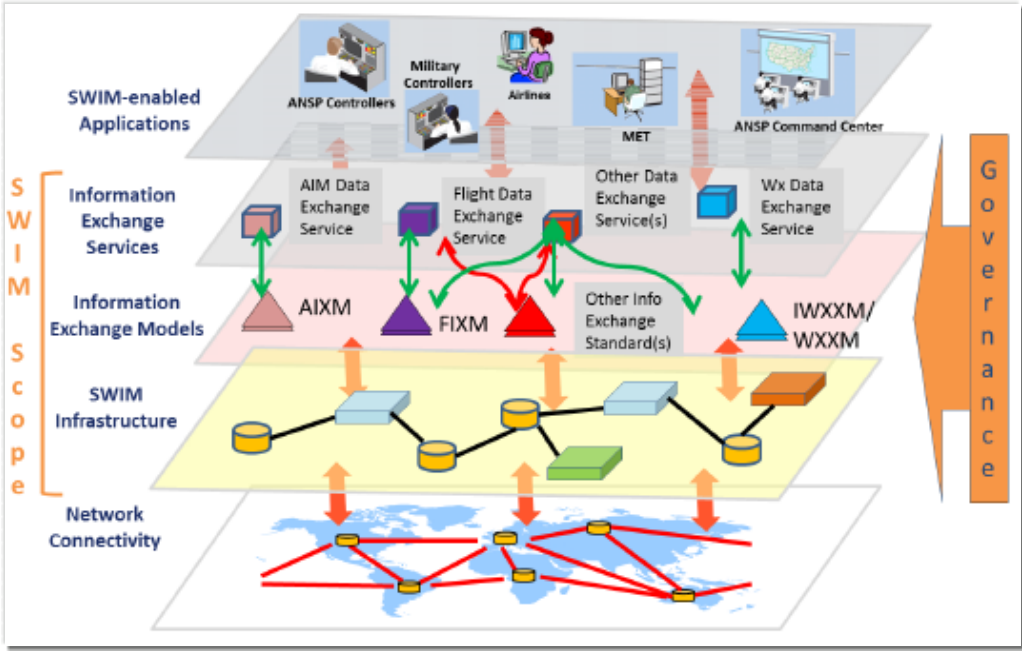
a) IT Systems perspective: Levels of IT Systems Interoperability (LISI) and PAID attributes



b) Data perspective: Levels of Conceptual Interoperability Model (LCIM)

End to End security & Security Risk Assessment (SRA)

- SWIM layered architecture introduces new primary and supporting assets.
- Primary assets: new and existing services offered via SWIM.
- Supporting assets:
  - (new and existing) System/application layer.
  - (new) SWIM infrastructure layer.
  - (new and existing) Network infrastructure layer (PENS, Internet).
- Evolution of existing and new supporting assets introduce new vulnerabilities but… (see next slide):
- SRA is performed for each layer.
- Integrated SRA: fan overall approach to security needs to be performed an end to end SRA, built as a consolidated composition of the layer based SRAs.

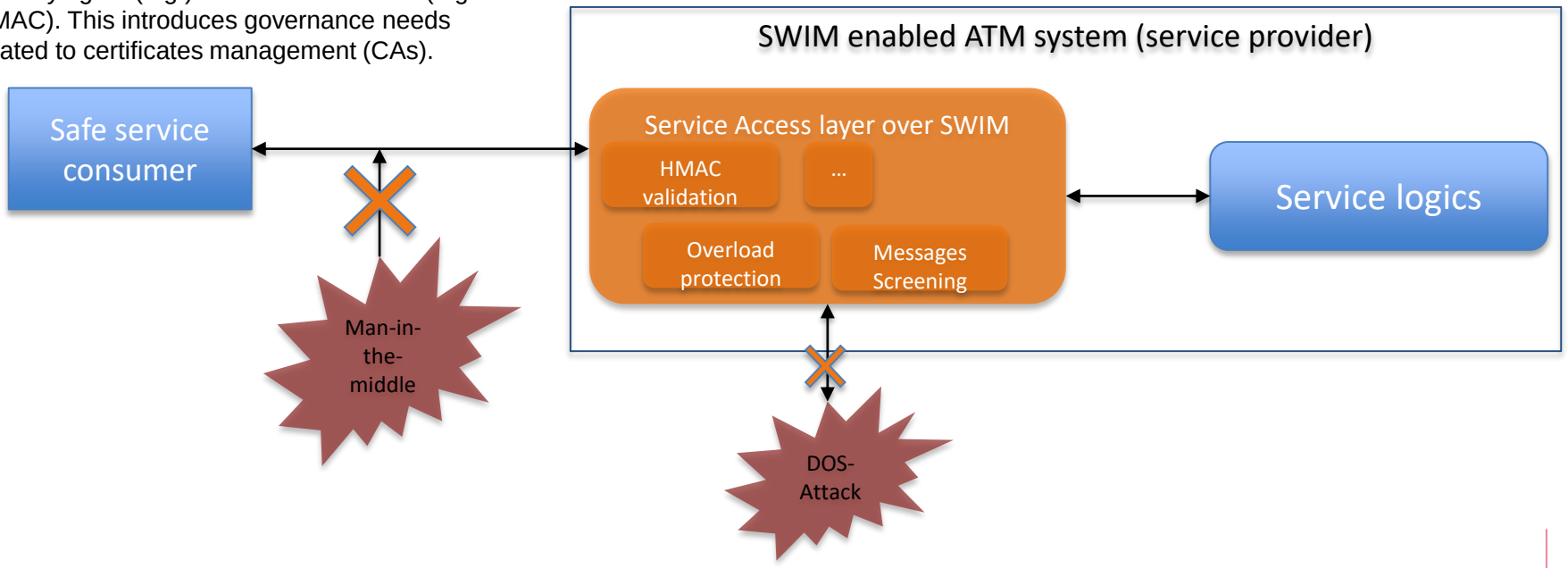


Ref. ICAO Doc 10039

End to End security & Security Risk Assessment (SRA)

- Evolution of existing and new supporting assets introduce new vulnerabilities but…:
  - SWIM infrastructure provides also Security Controls (SC) (e.g. overload protection) aiming at protecting application/system layer supporting assets.
  - Some SCs may be delegated to the SWIM infrastructure layer which implements such SCs in a standard way.

Message integrity and authenticity is protected by relaying on (e.g.) X.509v3 certificates (e.g. HMAC). This introduces governance needs related to certificates management (CAs).



Some Considerations on SWIM Security :

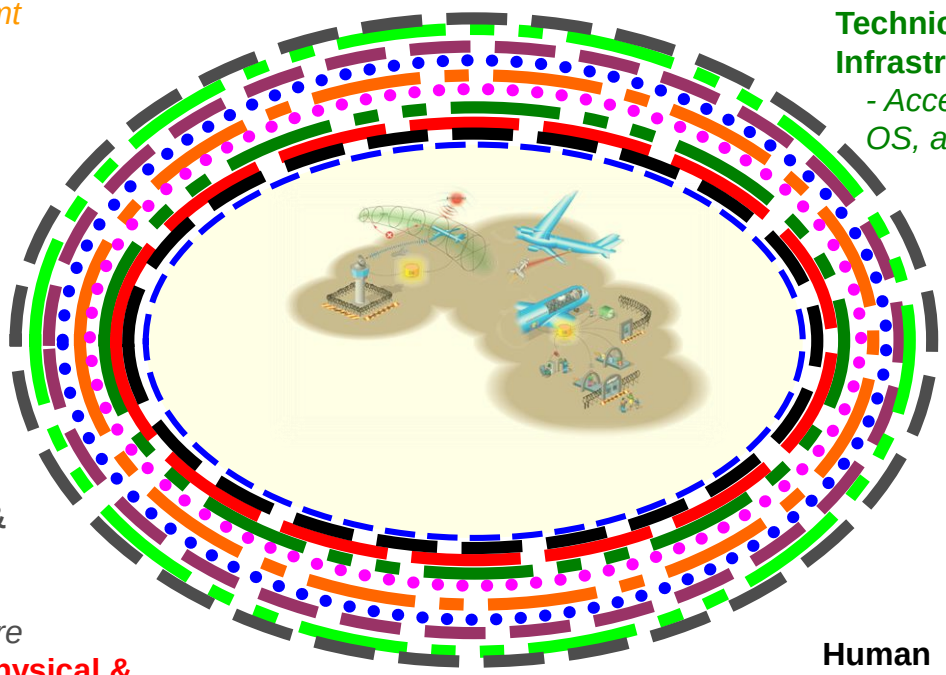
- Some SWIM layer SCs are based on two types of digital identities: X.509 certificates and Security tokens:
  - This introduces the needs of cross security domains trust relationships impacting the security management system.
  - This requires proper governance (e.g. trusted CAs, common certificate attributes, etc.)

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

Conclusions : Controls are not only Technology

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*

Monitoring & Audit
- *Logging*
- *Audits*

Physical & Environmental Security
- *Secure perimeter*
- *Equipment maintenance*
- *…*

SESAR 1-16.6.2 REFERENCE MATERIAL

Human Resources
- *Training*
- *Vetting*
- *…*

THANK **YOU** FOR YOUR ATTENTION

LEONARDO
SECURITY & INFORMATION SYSTEMS