International Council on Systems Engineering
A better world through a systems approach

SysML4Sec

Methodology for Security modeling in the context of large-scale product development with multiple design levels

Hartmut Hintze, Alice Santin,
Marvin Blecken, Daniel Patrick Pereira,
Ralf God

INCOSE International Symposium 2025 | Ottawa, Canada

Aircraft architectures are changing

YESTERDAY

Non-integrated aircraft

- Systems are simple, obscure, proprietary and isolated – clear ATA responsibilities
- easy integration, low complexity

TODAY

Integrated aircraft

- Systems share platforms (A653, Blades)
- Communication networks (Ethernet, AFDX)
- More complexity, more integration efforts

TOMORROW

eEnabled aircraft

- More and more COTS will be used
- Merging of ground and aircraft systems
- High integration complexity

Boeing 787 aircraft press review in 2008

The Register®

oftware | Music & Media | Comms | Security | Management | Sci

Crime | **Enterprise Security** | Anti-Virus | Spam | ID | Spyware

The Register » Security » Enterprise Security »

US regulator raises Dreamliner hacker risk fear

SICHERHEIT SECURITY-MANAGEMENT

Flugsicherheit

Boeings 'Dreamliner' anfällig für Hacker

Von: Liam Tung und Stefan Beiersmann

Montag, 7. Januar 2008

Die US-Flugaufsicht FAA hat Sicherheitsprobleme im Com Boeing 787 Dreamliner ausgemacht, weil dessen Unterha von der Bordelektronik abgekoppelt ist.

POLITICS : SECURITY

FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack

By Kim Zetter 01.04.08 | 7:30 PM

FOXNEWS.COM HOME > SCITECH

TECH TUESDAY

How to Hack Into a Boeing 787

Tuesday, February 19, 2008

By Jackson Kuhl
FOX NEWS

E-Mail | Print

Share: Digg | Facebook | StumbleUpon

Last month, technology news sites and blogs breathlessly reported on a Federal Aviation Administration document suggesting that Boeing's new 787 Dreamliner passenger jet may be vulnerable to computer hackers.

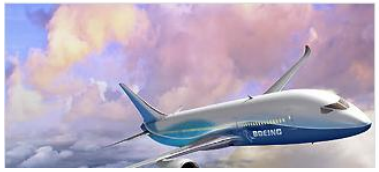
FOXNEWS.COM HOME > SCITECH

FAA: Terrorists Could Hack New Boeing Jetliner

Thursday, January 10, 2008

Associated Press

E-Mail | Print | Digg This! | del.icio.us



In-flight entertainment has come a long way since passengers craned their necks to catch a glimpse of the flickering films shown in 1980s aircraft.

Today's passengers expect on-demand video systems, telephones and even broadband Internet access

sueddeutsche.de

Home | E-Paper | Immobilienmarkt | Stellenmarkt | Motormarkt | Anzeigen | SZ-Sho

Politik | **Wirtschaft** | Finanzen | Kultur | Sport | Leben | Karriere | München | Bayern

09.01.2008 15:01 Uhr Drucken | Versenden | Kontakt

Der Dreamliner von Boeing
Foto: AFP

Boeing

Dreamliner auf Albtraum-Kurs

Mit wenigen Klicks zum Steuerknüppel: Die Bordcomputer des neuen Boeing-Flaggschiffs sind angeblich nicht ausreichend vor Hackerangriffen geschützt.

Von Wolfgang Koydl

Regulations Requirements for System Security

Published for Boeing 787:

Two Special Conditions from FAA (Federal Register, Dec. 28 2007):

- 25-07-01-SC: “The design shall prevent all inadvertent or malicious changes to, and all adverse impacts upon, all systems, networks, hardware, software, and data in the Aircraft Control Domain and in the Airline Information Domain from all points within the Passenger Information and Entertainment Domain.”

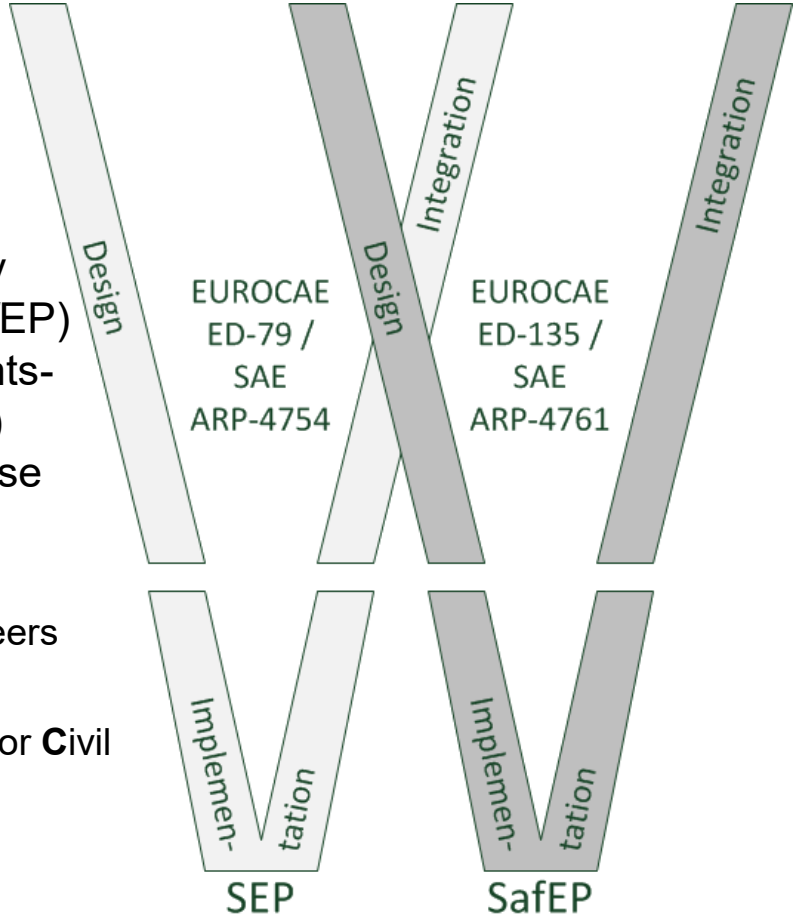
- 25-07-02-SC: “The applicant shall ensure system security protection for the Aircraft Control Domain and Airline Information Services Domain from access by unauthorized sources external to the airplane. The applicant shall also ensure that security threats are identified and assessed, and that risk mitigation strategies are implemented to protect the airplane from all adverse impacts on safety, functionality, and continued airworthiness.

From to the Two-V-Model …

The System Engineering process (SEP) and Safety Engineering Process (SafEP) are using the Requirements-Based Engineering (RBE) method at the design phase today.

SAE –
Society of **A**utomobile **E**ngineers

EUROCAE –
The **Eur**opean **O**rganization for **C**ivil **A**viation **E**quipment



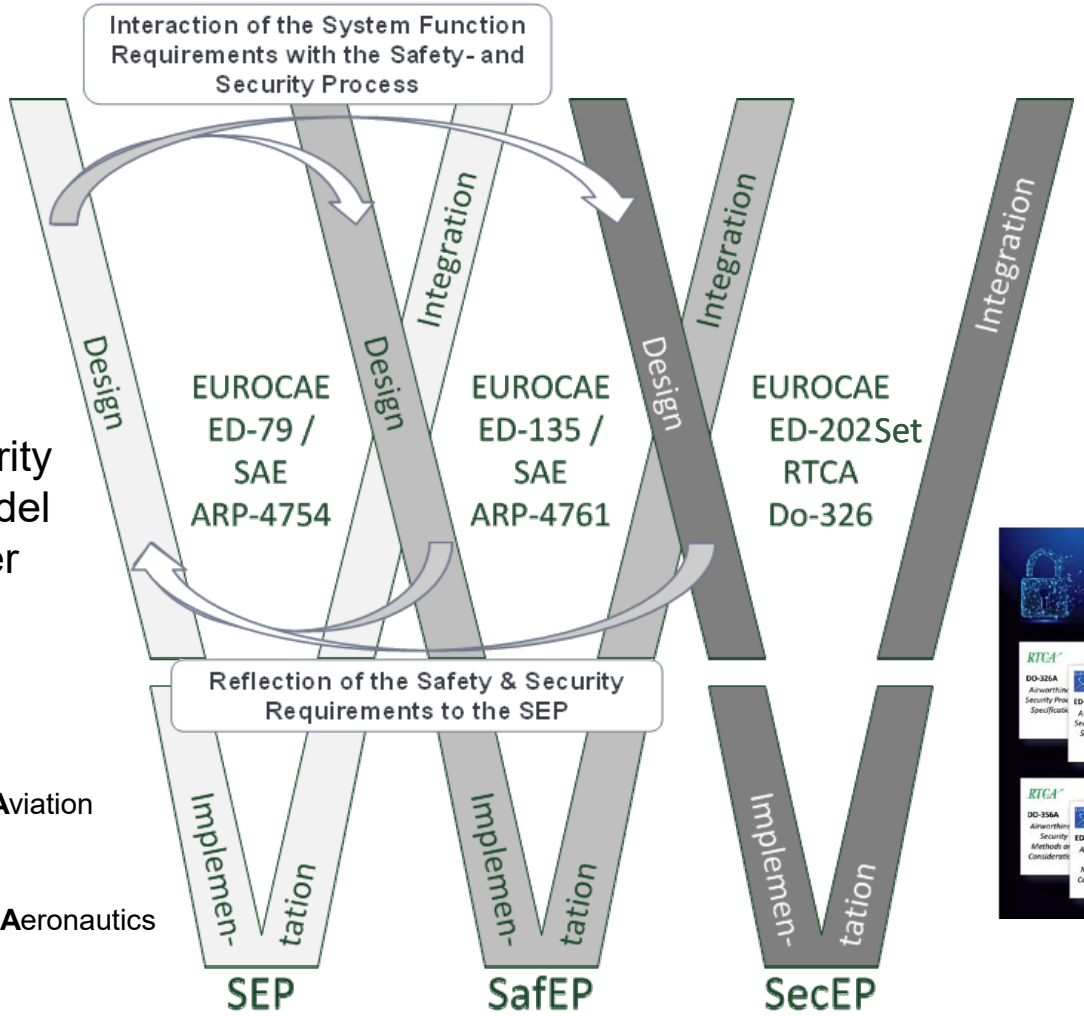
… to the Three-V-Model

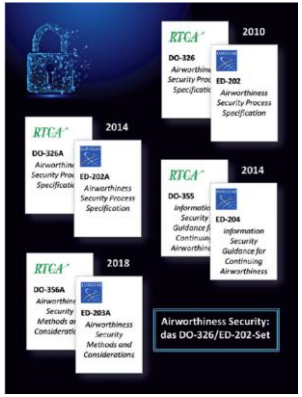
The Two-V-Model was extended by the Security Engineering Process (SecEP) to fulfil the authority requirements. Each V-Model is interacting with the other ones.

SAE –
Society of **A**utomobile **E**ngineers

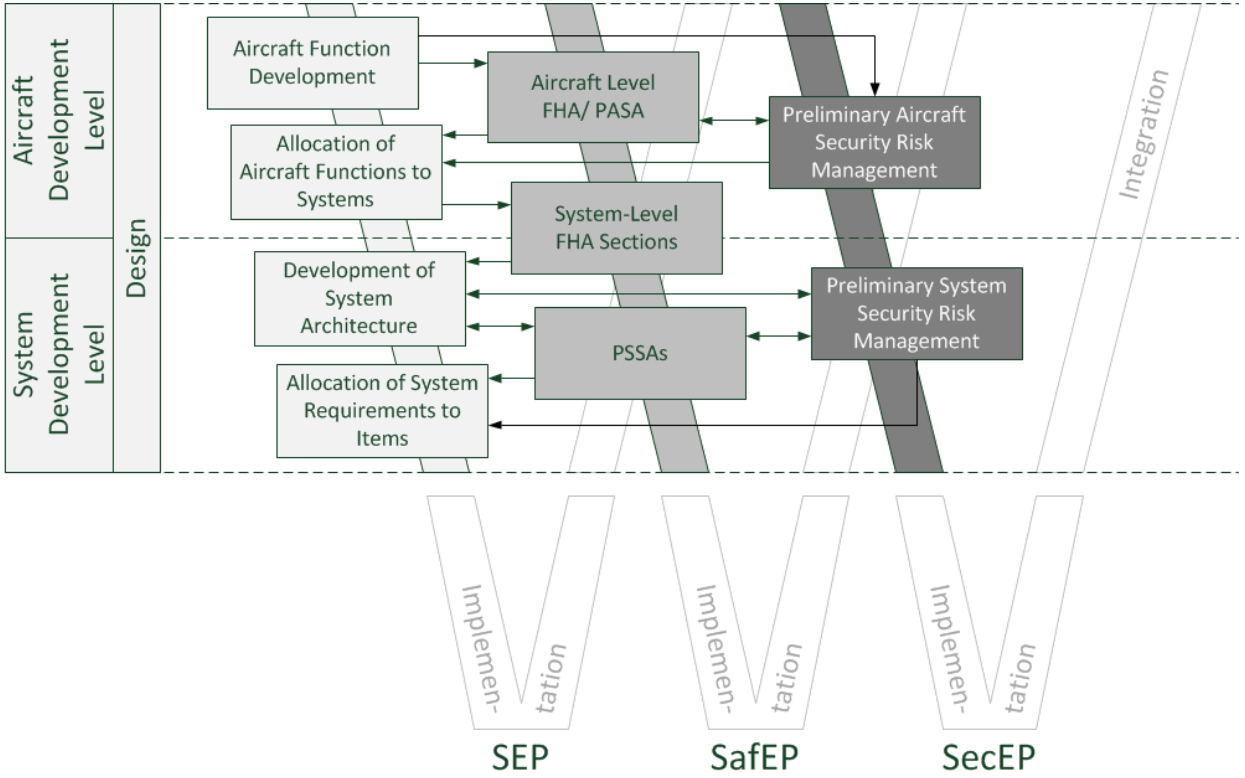
EUROCAE –
The **Eur**opean **O**rganization for **C**ivil **A**viation **E**quipment

RTCA –
The **R**adio **T**echnical **C**ommission for **A**eronautics

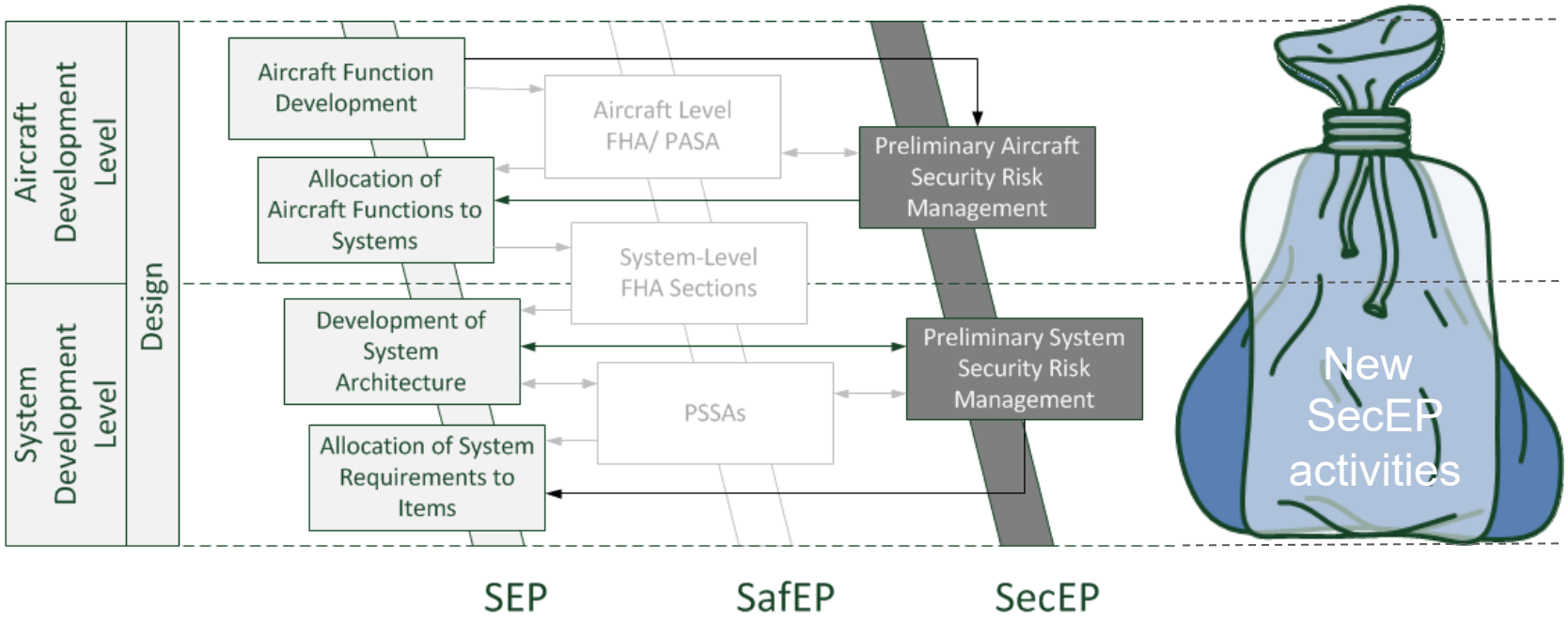




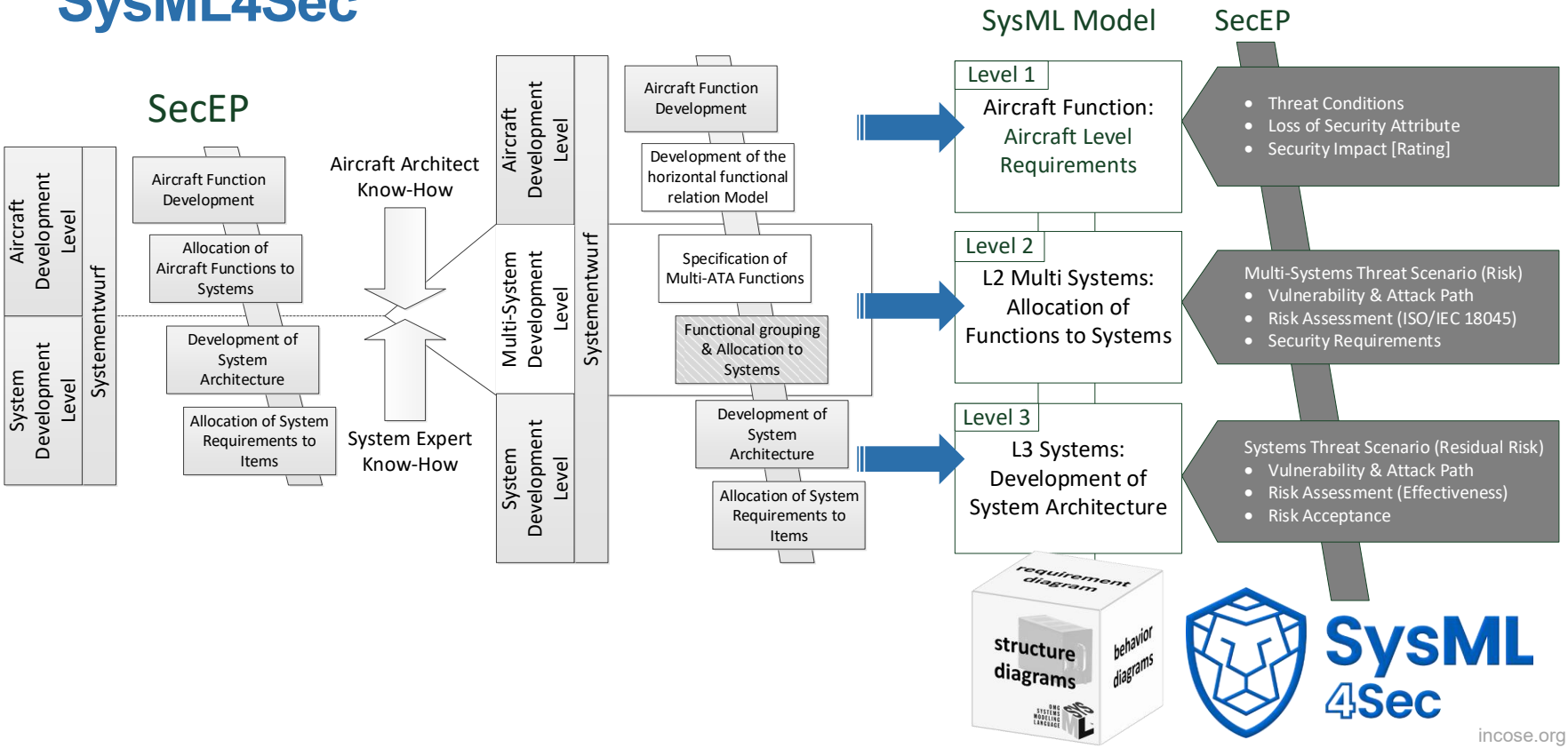
Detailed activities of the Three-V-Model Design phase specified by SAE ARP- 4754



Focusing on the SEP & SecEP for the new process approach



SysML4Sec


SecEP
Aircraft Development Level
System Development Level
Systementwurf
Aircraft Function Development
Allocation of Aircraft Functions to Systems
Development of System Architecture
Allocation of System Requirements to Items
Aircraft Architect Know-How
System Expert Know-How
Aircraft Development Level
Multi-System Development Level
System Development Level
Systementwurf
Aircraft Function Development
Development of the horizontal functional relation Model
Specification of Multi-ATA Functions
Functional grouping & Allocation to Systems
Development of System Architecture
Allocation of System Requirements to Items
SysML Model
SecEP
Level 1
Aircraft Function: Aircraft Level Requirements
Threat Conditions
Loss of Security Attribute
Security Impact [Rating]
Level 2
L2 Multi Systems: Allocation of Functions to Systems
Multi-Systems Threat Scenario (Risk)
Vulnerability & Attack Path
Risk Assessment (ISO/IEC 18045)
Security Requirements
Level 3
L3 Systems: Development of System Architecture
Systems Threat Scenario (Residual Risk)
Vulnerability & Attack Path
Risk Assessment (Effectiveness)
Risk Acceptance
requirement diagram
structure diagrams
behavior diagrams
SysML 4Sec

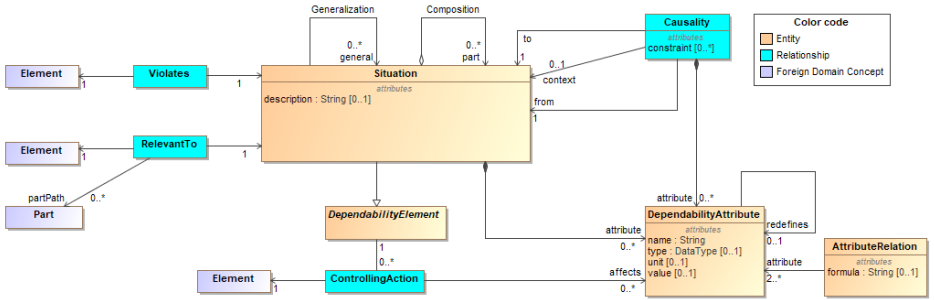
RAAML | A safety and cybersecurity modeling language (1/2)

- **OMG RAAML 1.0 FTF:**
  - Extensions to SysML needed to support safety and reliability analysis
  - Published in April 2023

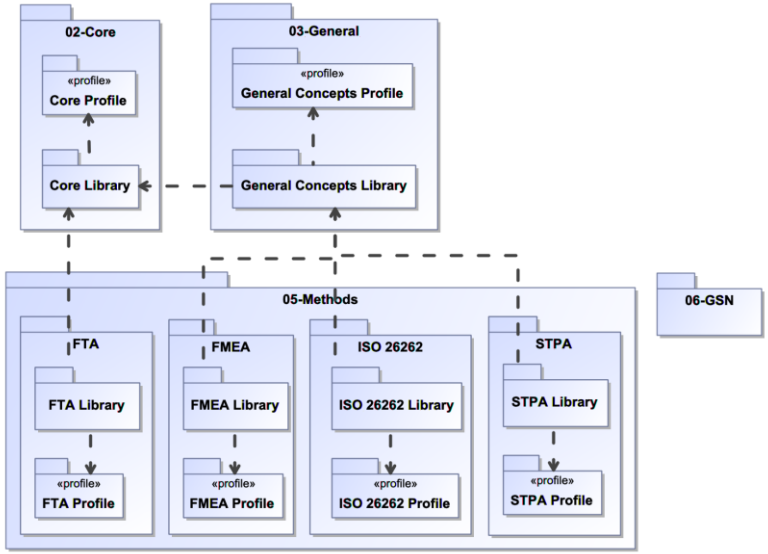
OMG Object Management Group.

RAAML
OMG RISK ANALYSIS AND ASSESSMENT MODELING LANGUAGE

Core concepts domain model



Methods



Main Contributors

Ford · AEROSPACE · AIRBUS · DASSAULT SYSTEMES · MITRE · National Institute of Advanced Industrial Science and Technology AIST · GfSE · cea

RAAML | A safety and cybersecurity modeling language (2/2)

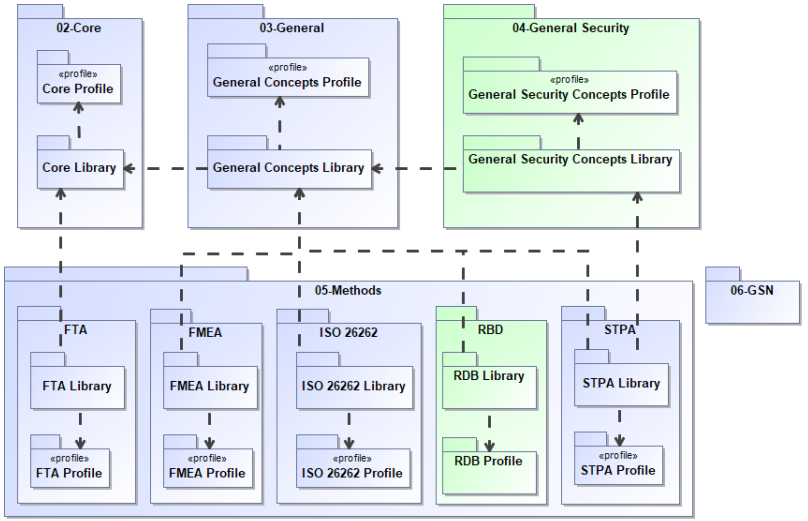
- **OMG RAAML 1.1, beta version available since June 2024**
  - Foundations for security to support specific security method (e.g. TARA ISO21434, STPA-Sec)
  - Reliability Block Diagrams (RDB)

- New concepts (common & security specific):
  - Item
  - Asset (with value attributes – various *-ilities)
  - Loss, Impact (with individually rated impact to each attr
  - Factor (promoted from STPA)
  - Limitation, Weakness, Vulnerability
  - Threat, Threat Actor (Security-Specific)

Main Contributors

Ford, AEROSPACE, AIRBUS, DASSAULT SYSTEMES, MITRE, TUHH Hamburg University of Technology

Methods



SysML-based & multi-systems risk assessment for aviation

System Engineer

Security Engineer

L1 Aircraft Function

Aircraft functional architecture

- Security Assets
- Indirect Assets
- Flight Phases
- Use Cases
- Misuse Cases

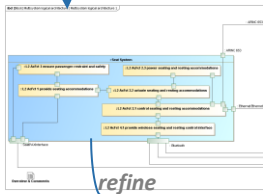
refine

- **Threat Conditions**
- Loss of Security Attribute
- Security Impact

#	Name	Security Attribute	Aggregate Impact Rating
1	TC-27 L1 AcFct 2 provide resting accommodations Accountability Impact	Accountability	No Effect
2	TC-28 L1 AcFct 2 provide resting accommodations Availability Impact	Availability	Major
3	TC-29 L1 AcFct 2 provide resting accommodations Confidentiality Impact	Confidentiality	No Effect
4	TC-30 L1 AcFct 2 provide resting accommodations Integrity Impact	Integrity	Major
5	TC-31 L1 AcFct 2 provide resting accommodations Privacy Impact	Privacy	No Effect

L2 Multi Systems

Logical & Functional architecture (IBD)



refine

Multi-Systems Threat Scenario [Risk]

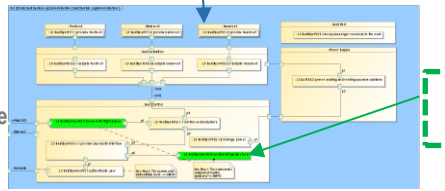
- Vulnerability & Attack Path
- Risk assessment as per ISO 18 045:2022
- Security Requirements

Risk Acceptability

	Severity of the Threat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

L3 Systems

Logical & functional architecture (IBD)



satisfy

Security Measures

Systems Threat Scenario [Residual Risk]

- Refine Multi-Systems Threat Scenario
- Vulnerability & Attack Path
- Risk Assessment as per DO326 Effectiveness method
- Risk Acceptance

Effectiveness Matrix

System de

Security Risk Assessment

Workflow for model-based Airworthiness security assessment

L1 – Aircraft Level | L2 - Multi-systems level | L3 - Systems level

System Engineer

1

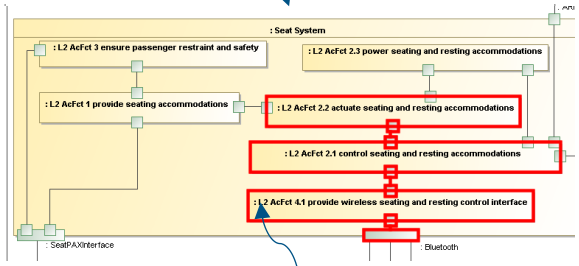
Design Aircraft functional architecture.
Define ***Flight phase*** and ***Indirect Asset*** (Crew, Passengers…)

2

Identify relevant Aircraft functions as ***Security Assets***

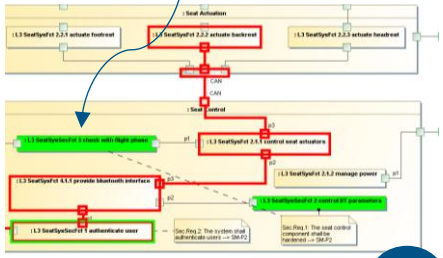
4

Design Logical and Functional architecture



7

Refine Logical and Functional architecture adding ***Security Measures***



Security Engineer

3

Create ***Threat Condition*** table for each ***Security Asset*** and rate its ***Impact*** on ***Indirect Assets***

#	Name	Security Attribute	Threat Condition	Aggregate Impact Rating	Impact On 'Airline'	Rationale for Rating of Impact On 'Airline'
1	TC-1 L1 AcFct 2 provide resting a	Accountability	TC-1 L1 AcFct 2 provide re	No Effect	No Effect	The *rational* is that one…
2	TC-2 L1 AcFct 2 provide resting a	Availability	TC-2 L1 AcFct 2 provide re	Major	No Effect	
3	TC-3 L1 AcFct 2 provide resting a	Confidentiality	TC-3 L1 AcFct 2 provide re	No Effect	No Effect	
4	TC-4 L1 AcFct 2 provide resting a	Integrity	TC-4 L1 AcFct 2 provide re	Major	No Effect	
5	TC-5 L1 AcFct 2 provide resting a	Privacy	TC-5 L1 AcFct 2 provide re	No Effect	No Effect	

5

Create ***Attack Path*** directly on the system model and rate its ***likelihood***

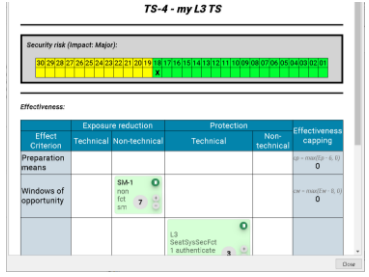
6

Create ***Pre-Threat Scenario*** including ***Threat Source***, ***Vulnerability, Attack Path, Threat Condition. Risk Acceptability*** *is automatically derived*
Create ***Security Requirements*** *for unacceptable risk*

#	Threat Source	Name	Lower Level Threat Scenario	Vulnerability	Attack Path	Misuse Case	Threat Condition	Aggregated Impact Rating	Likelihood	Risk	Requirement
1	human with intention	MultiSystems TS-1 Tampering of Seat accomodation for resting through Seat Bluetooth	TS-4 System TS1	AV1- Seat Bluetooth interface	AP-1 Spoofing through Seat Bluetooth	MUC-1 MUC1 - Adjust seat of other passengers	TC-2B L1 AcFct 2 provide resting accommodations Availability Impact TC-3B L1 AcFct 2 provide resting accommodations Integrity Impact	Major	4	Unacceptable	1 Prevent tampering of seat accomodation for resting through Seat Bluetooth
2	human with intention	MultiSystems TS-2 Tampering of Seat accomodation for resting through Entertainment Bluetooth		AV2- Entertainment Bluetooth interface	AP-2 Spoofing through Entertainment Bluetooth	MUC-1 MUC1 - Adjust seat of other passengers	TC-2B L1 AcFct 2 provide resting accommodations Availability Impact TC-3B L1 AcFct 2 provide resting accommodations Integrity Impact	Major	11	Unacceptable	2 Prevent tampering of seat accomodation for resting through Entertainment Bluetooth

8

Based on ***Pre-Threat Scenario***, create ***Post -Threat Scenario*** that refined ***Attack Path*** including new ***Security Measures.*** Rate ***Effectiveness*** to get ***Risk Acceptability*** result.



KEY TAKE AWAYS

SysML 4Sec

SECURITY BY DESIGN

Integrated Security : people agnostic, no ambiguity, fully connected to the model

TRACEABILITY

Multi-systems level where High level design is connected to Lower levels solutions

Secure from Design to Certication

CONSISTENCY

Iterative assessment to adapt to the system design level

Customizable to follow standards & best practices evolution

SCALABILITY

Knowledge sharing collaborative work between systems and security engineers

Thank You!

Hartmut Hintze
Hamburg University of Technology
Hein-Saß-Weg 22, D-21129 Hamburg
Hartmut.Hintze@TUHH.de

Overview Today's Regulations and Standards