STAMP/STPA - A Systems Theory Approach to Analyze Security Concerns

Dr. Daniel Patrick Pereira

Cyber security Architect for Commercial and Military aircrafts

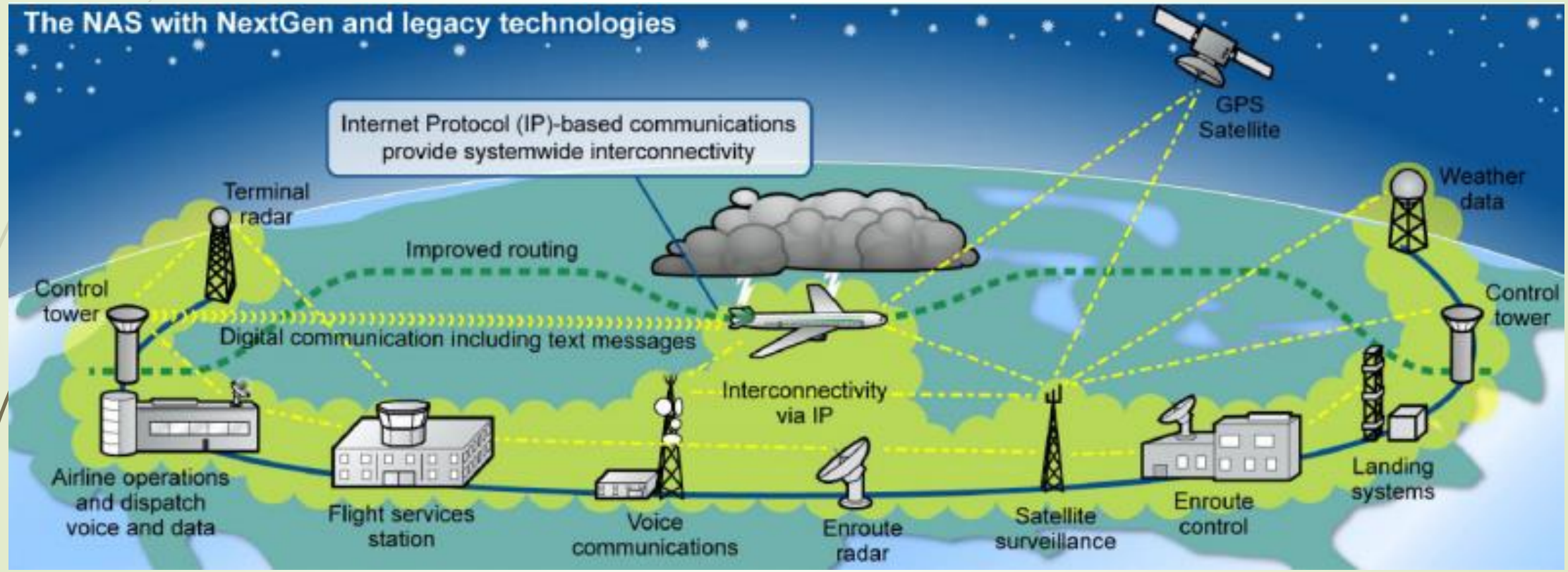
Airbus Defence & Space

May/2022

Agenda

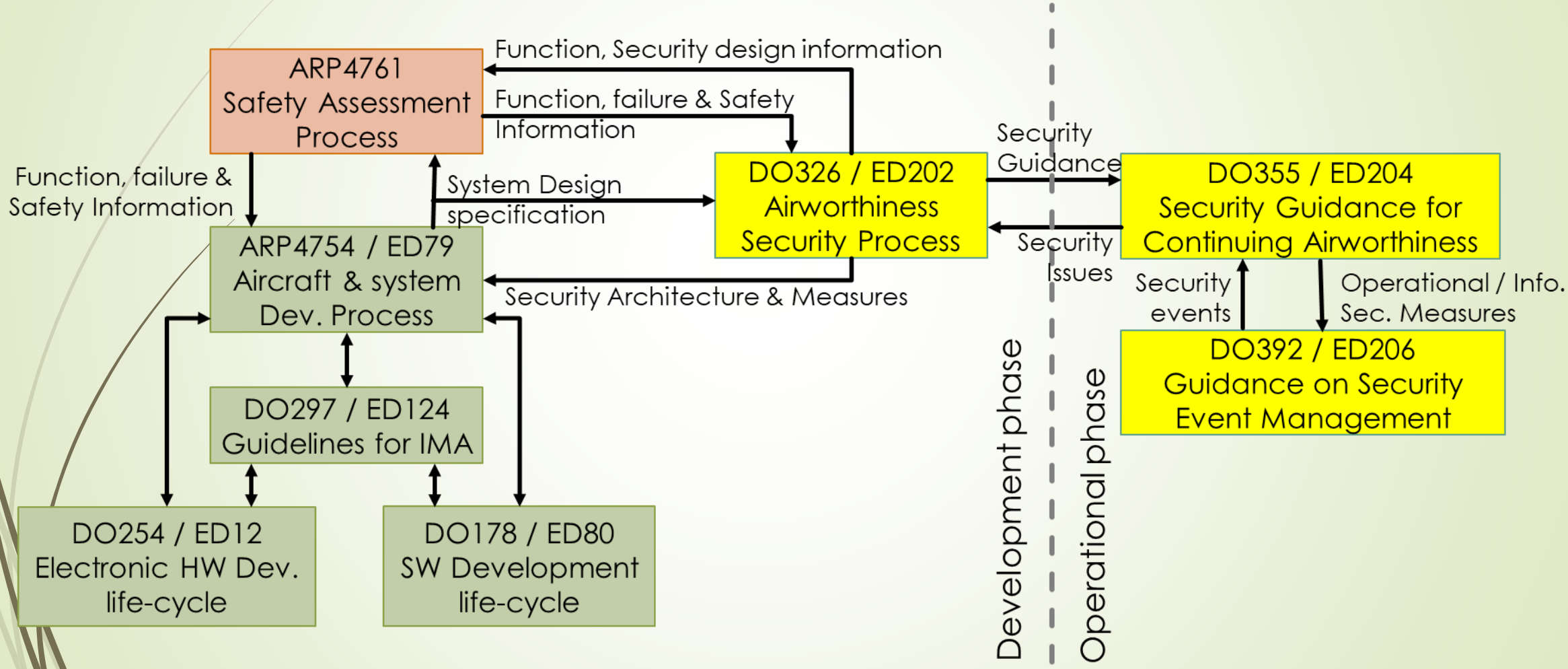
1. Problem
2. ED-202A / ED-203A
3. STAMP/ STPA
4. Case study
5. Reference

Increasing complexity

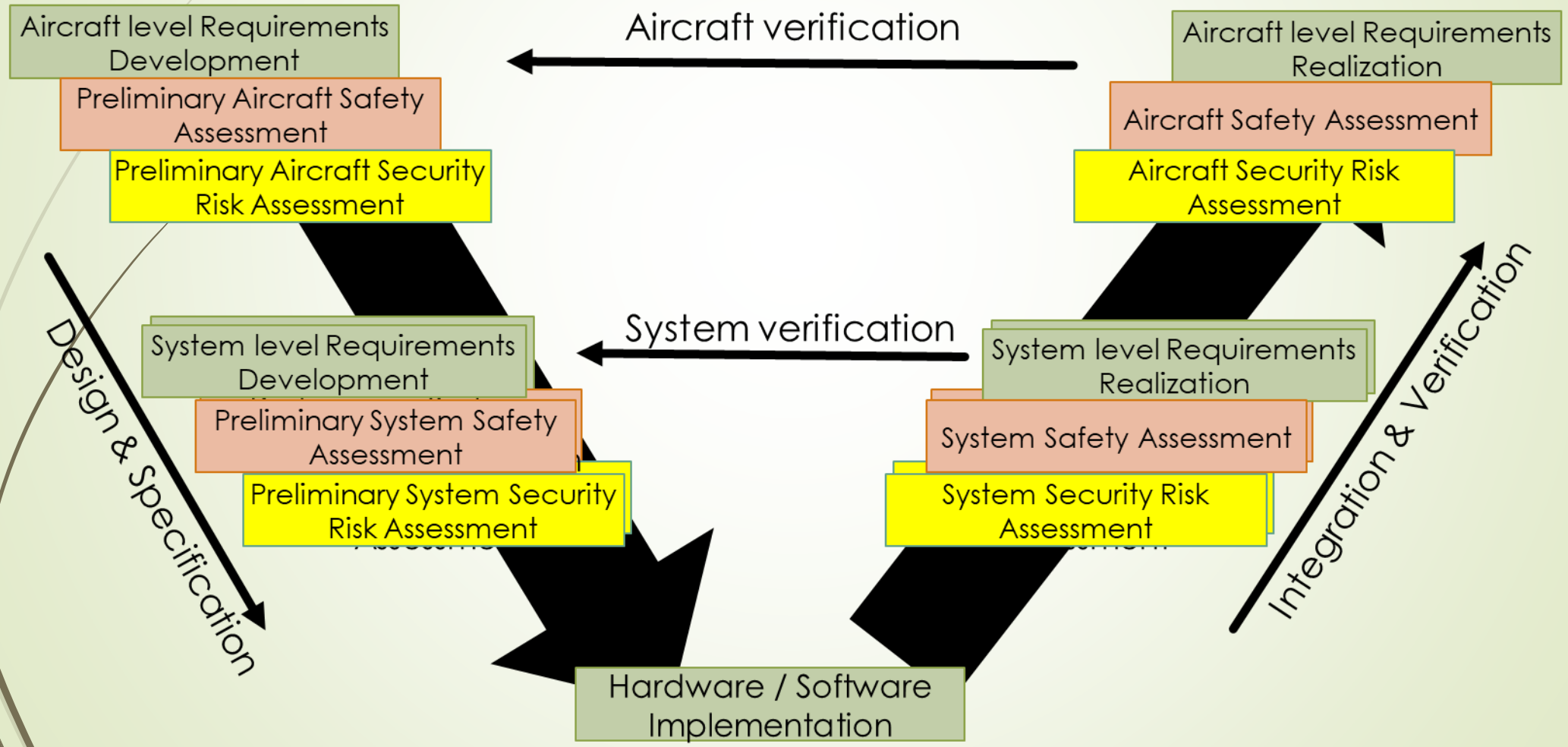


Source: NASA/CR–2015 - Operatic Analysis of Distributed Systems.

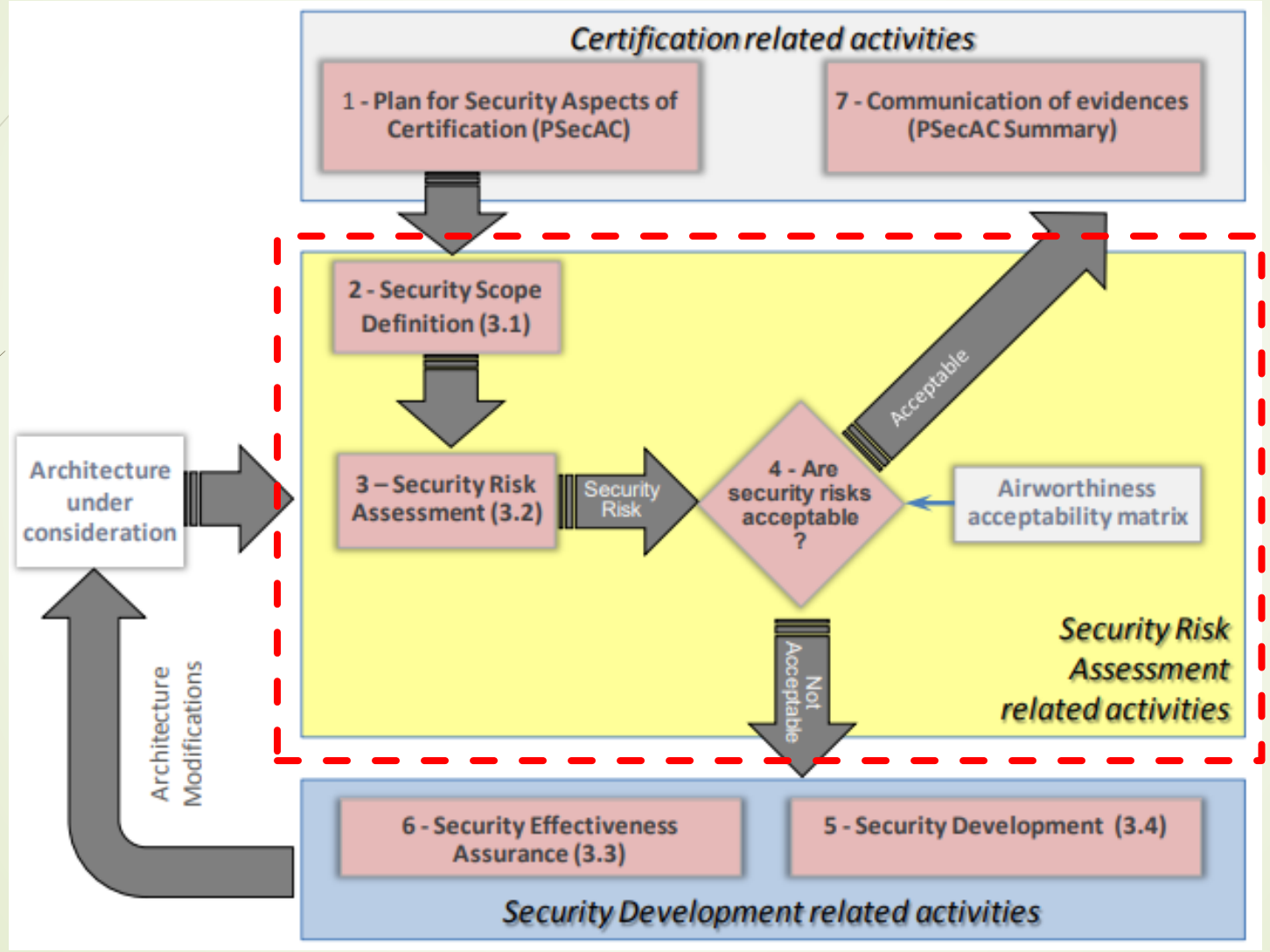
Aeronautical standards



Aeronautical standards (V-Model)

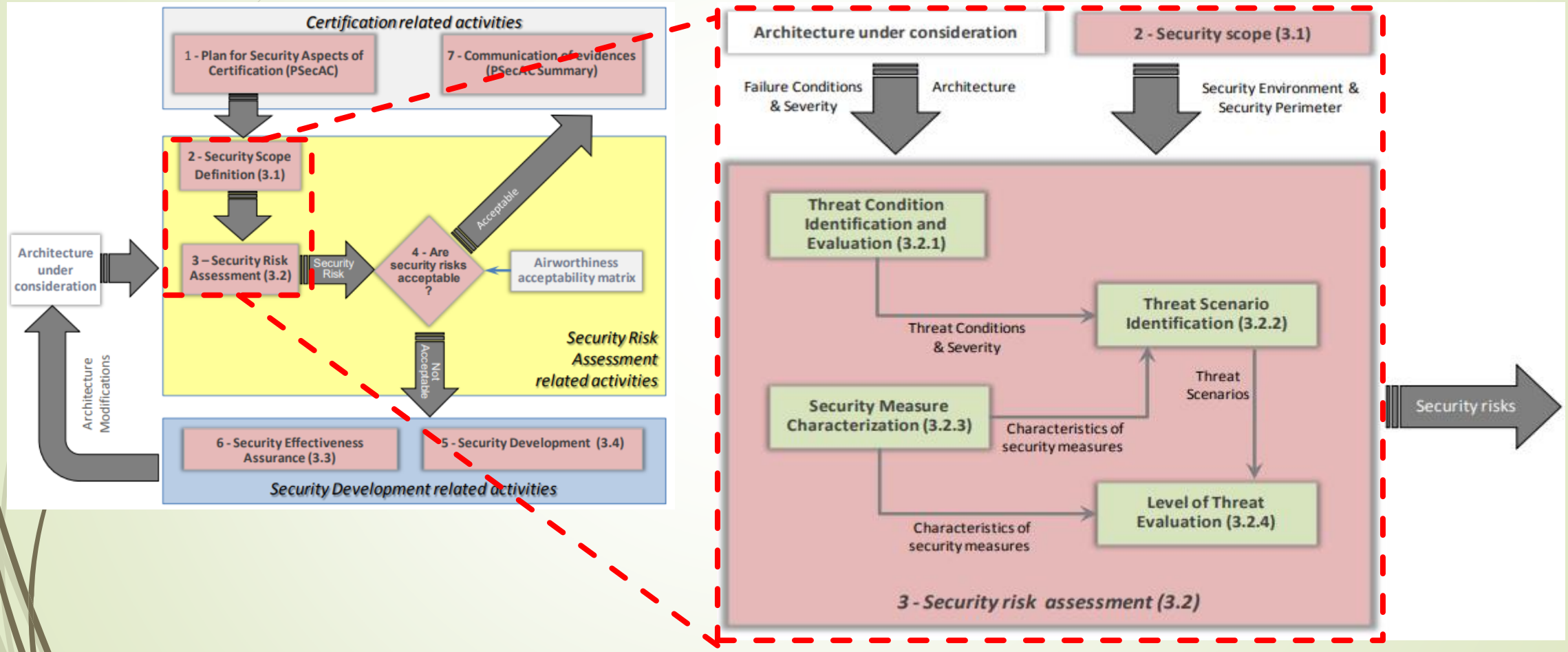


DO326A / ED202A



Source: RTCA DO-326A Airworthiness Security Process Specification

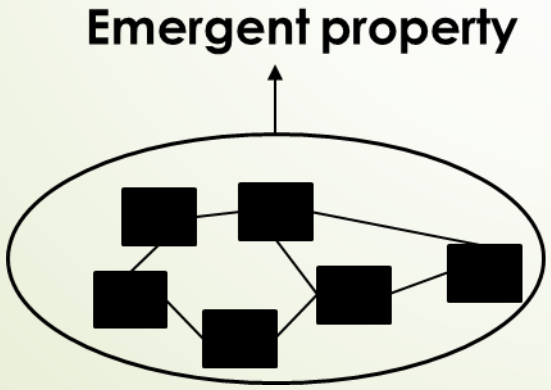
DO326A / ED202A – Security Risk Assessment

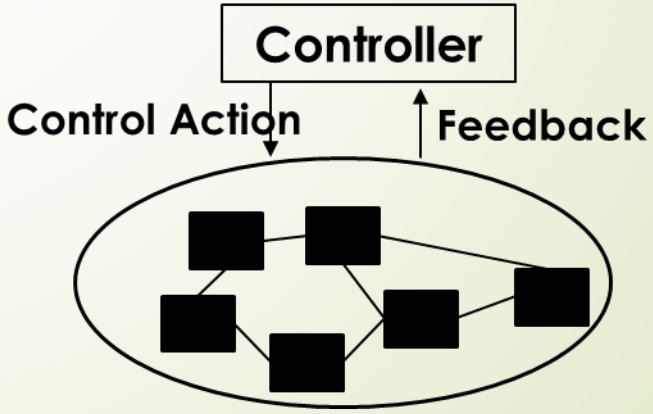


Source: RTCA DO-326A Airworthiness Security Process Specification

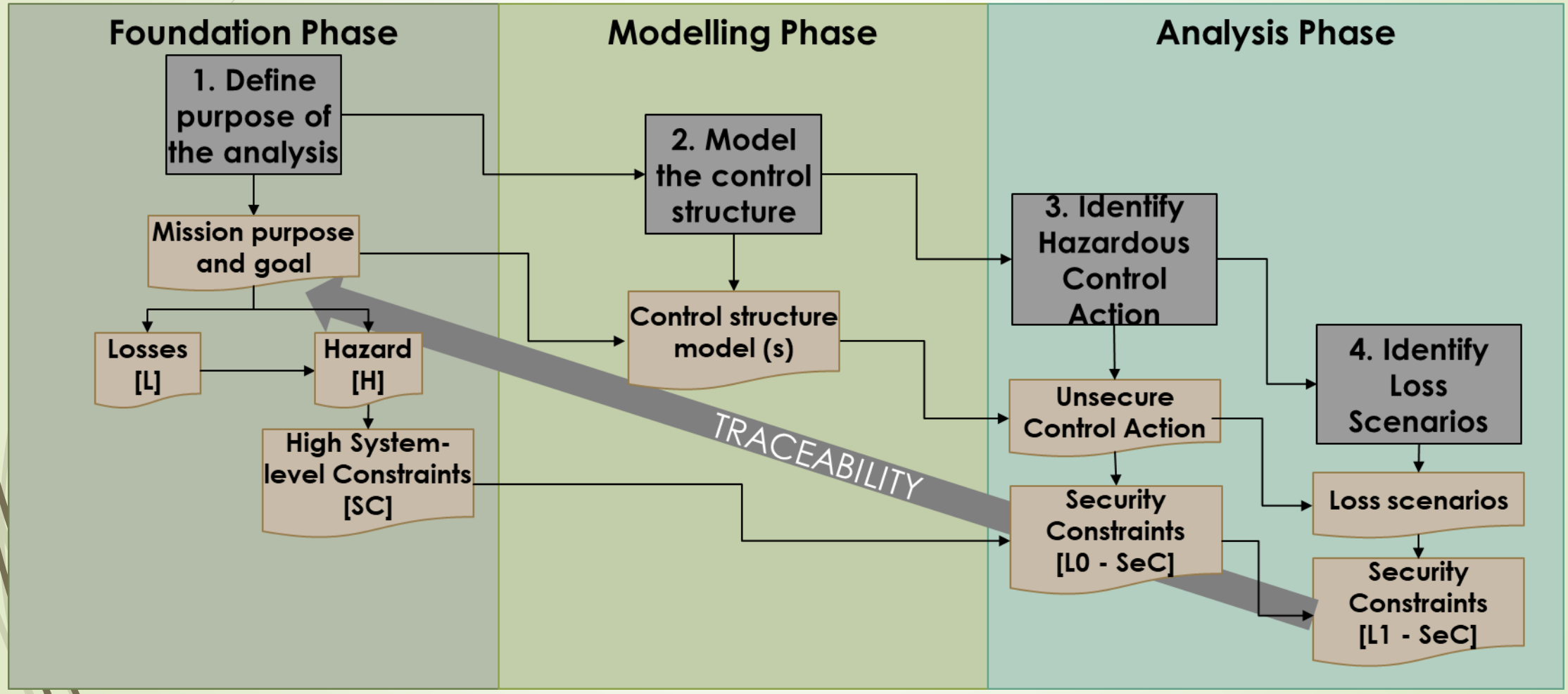
STAMP/STPA for Security

- **S**ystem **T**heoretic **A**ccident **M**odel and **P**rocess is an accident causality model based on Systems Thinking / Systems Theory and Control Theory concepts;
- **S**ystem-**T**heoretic **P**rocess **A**nalysis is a top-down system engineering technique based on STAMP for security and mission assurance analyzes;
- The **accident causation** is expanded beyond failure events, including the entire social-technical system, components interaction accidents, human errors, software and system design errors.

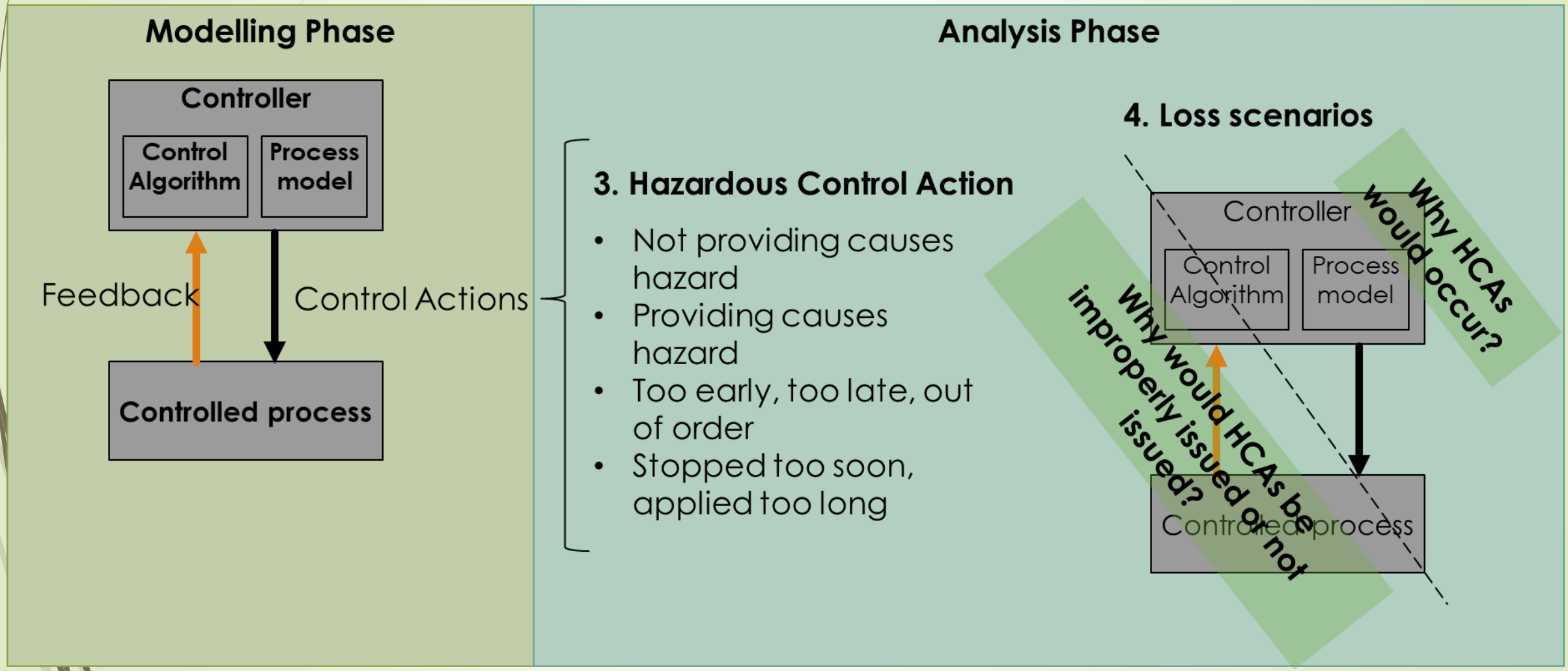




Basic Steps of STPA for security



STPA for security – Modelling / Analysis Phases



DO326A / ED202A vs STPA for Security

DO326A / ED202A	STPA for Security
Security scope definition • Identification of Assets • Definition of security perimeter • Specification of security environment	**Foundation phase** 1. Define purpose of the analysis **Modelling phase** 2. Model the control structure
Security Risk Assessment • Threat condition identification and evaluation • Threat scenario identification	**Analysis phase** 3. Identify hazardous control action 4. Identify loss scenarios
• Security measure characterization • Level of threat evaluation	

Use Case – Flight Management System

- Mission purpose and goal
  - A system to provide
    - **uninterrupted, aircraft current state and route from departure airport to the destination airport**
  - through
    - **multi sensor position and velocity data, navigation database, and communication**
  - in order to
    - **give navigation function location, frequency, elevation, and class information for the various ground-based radio navigation systems**

Use Case – Flight Management System

- Losses and Hazards

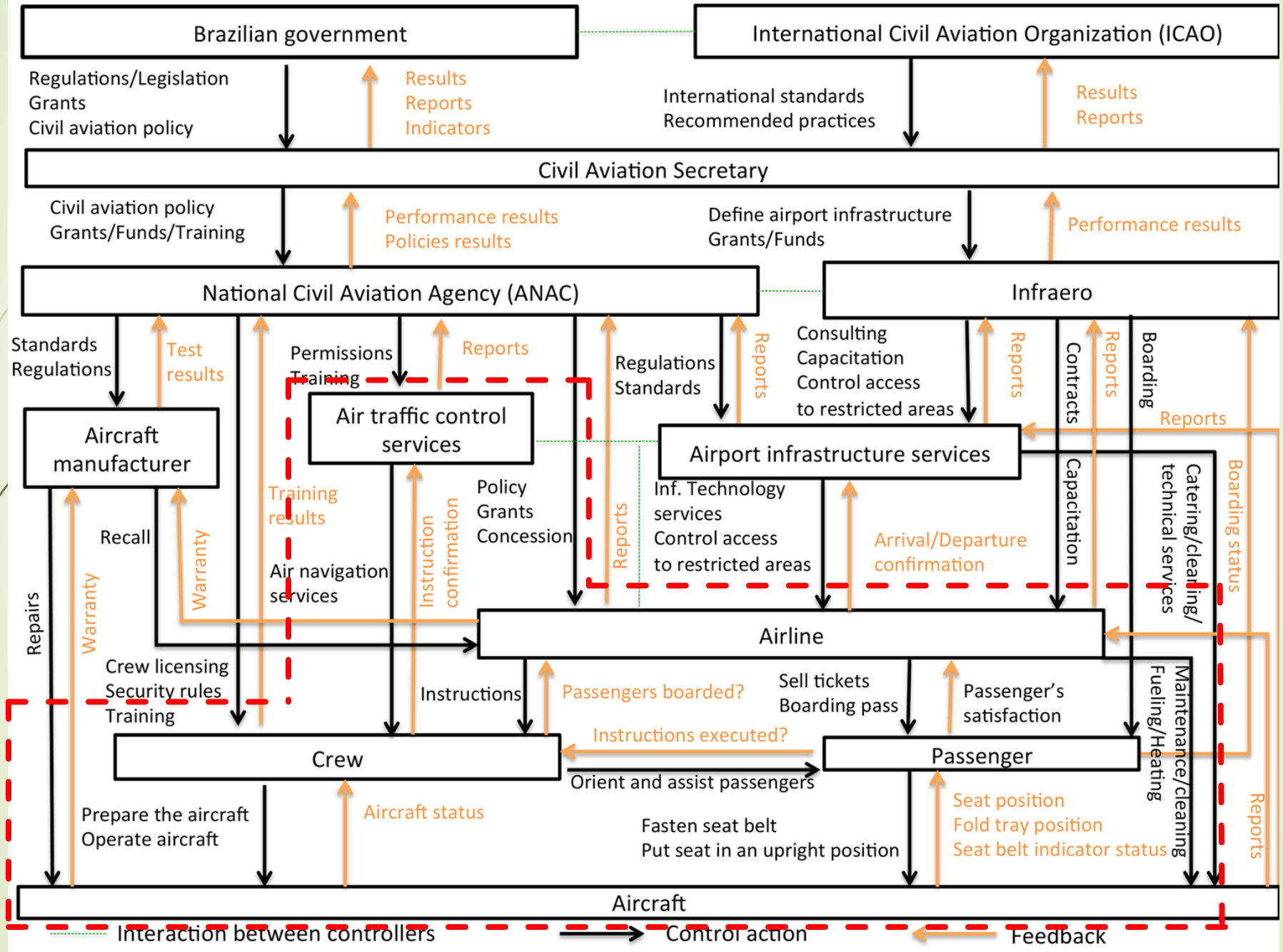
A **loss** involves something of value to stakeholders.

A **hazard** is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.

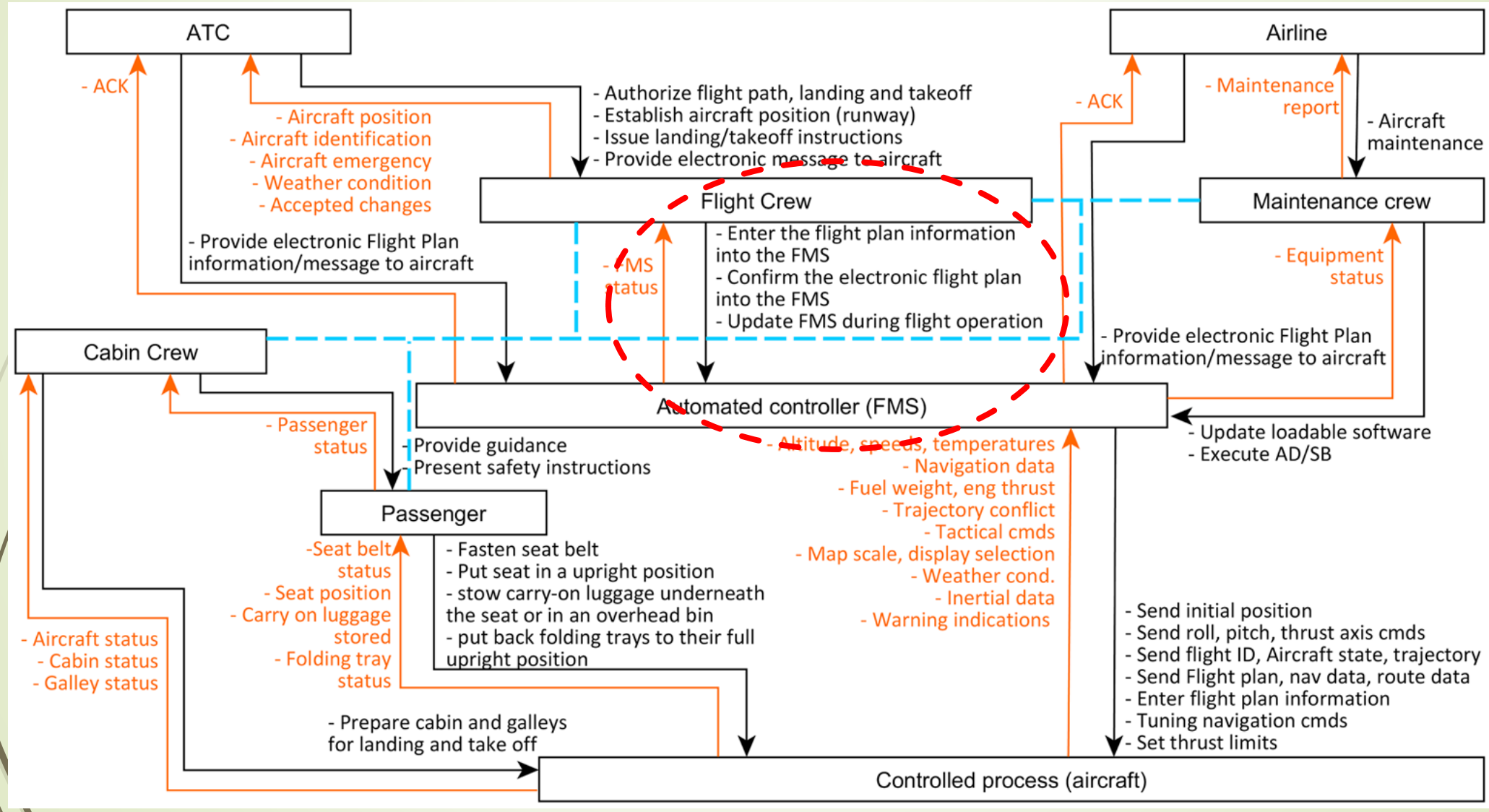
	L1: Loss of life/serious injury	**L2**: Loss of personal identifiable information (PII)	**L3**: Loss of credibility in the air transportation industry	**L4**: Aircraft damage
H1: Violation of minimum/maximum altitude	X		X	X
H2: Violation of minimum distance to other aircraft	X		X	X
H3: Uncontrolled aircraft	X		X	X
H4: Aircraft flying off the route specified at flight plan	X		X	X
H5: Unauthorized access to aircraft equipment (electronic and physical)	X	X	X	X
H6: Unable to dispatch aircraft			X	

Foundation Phase	Modelling Phase	Analysis Phase	Analysis Phase
1. Define purpose of the analysis	2. Model the control structure	3. Identify hazardous control action	4. Identify loss scenarios

Use Case – Flight Management System



Use Case – Flight Management System



Use Case – Flight Management System

- Control Action (Flight crew → FMS): Enter **flight plan** information into the FMS

Hazardous Control Actions	**Security Constraints (L0)**
[13] Not providing "Enter **flight plan** information into the FMS" when flight plan information is available. [H6]	**Cockpit crew** must be able to enter flight plan information.
[14] Providing "Enter **flight plan** information into the FMS" when flight plan information is tampered or faked. [H1, H2, H3, H4]	**Flight Plan** information must not be tampered or faked.
[15] Providing "Enter **flight plan** information into the FMS" too late when flight plan information is available. [H6]	**Cockpit crew** must be able to enter flight plan information.

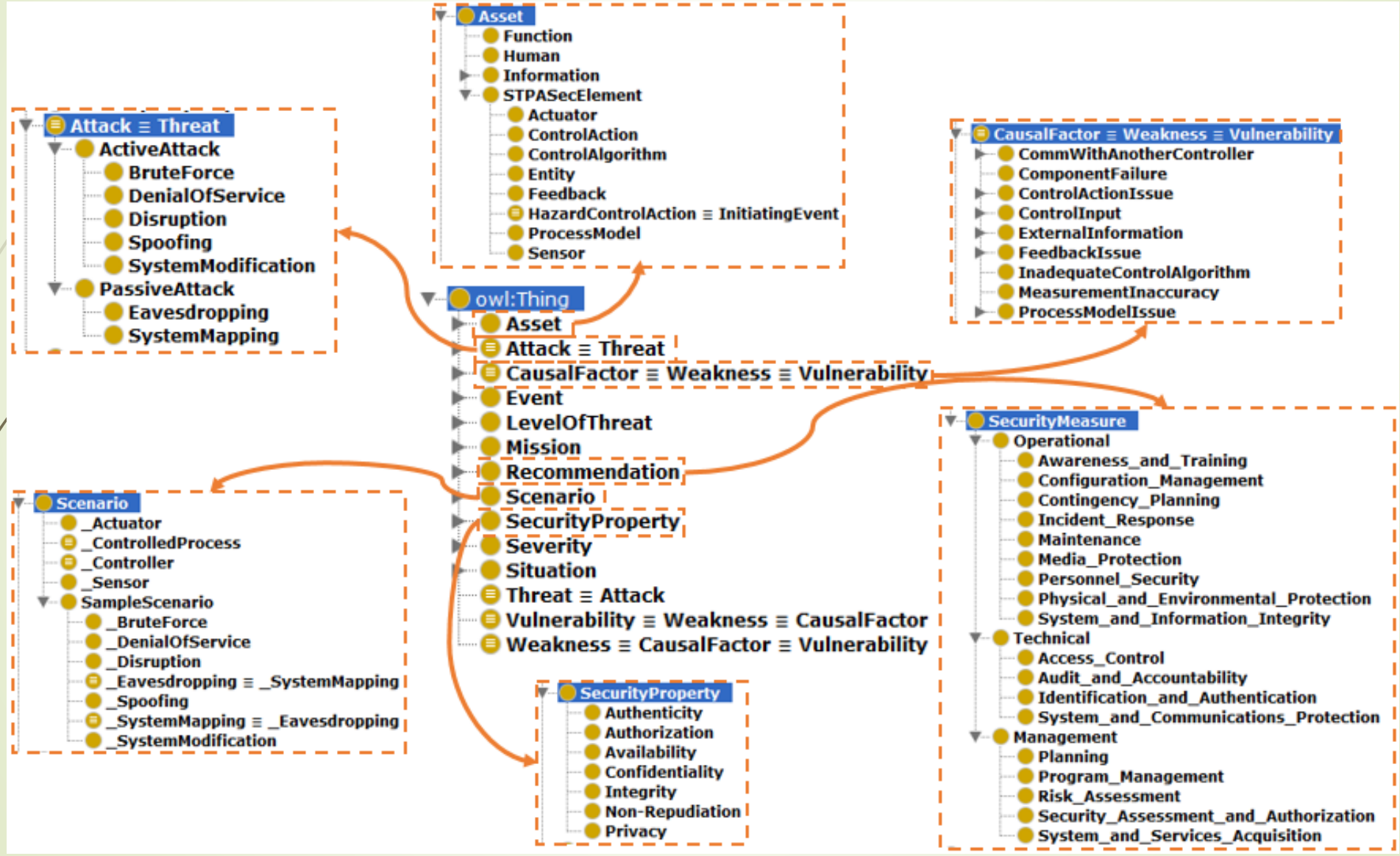
Use Case – Flight Management System

- Scenario

HCA 14: Flight crew provides **"enter flight plan information into the FMS"** when flight plan information is **tampered** or **faked**.

Scenarios	Security Causal Factors	D4 Evaluation (Goal impact)	Security Constraints (L1)
Fake flight plan information is provided to flight crew [external information wrong]	5. Flight plan information can be intercepted and modified. 6. Flight plan information is not protected. 7. Communication channel is not protected.	**Duration**: Permanent **Extent**: Total (**Destroy**)	• Paper based flight plan must be numbered, signed, … • Communication channel must authenticate before start transmit/receive. • FMS system must encrypt the data.
Correct flight plan information is provided, but mistakes are made by the flight crew when entering its information into the FMS	8. Some fields on the paper based flight plan are illegible	**Duration**: Permanent **Extent**: Total (**Destroy**)	• Paper based flight plan must not have hand-written information

STPA Ontology



References

- Leveson, N. and Thomas, J. P., 2018. **STPA Handbook**. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- Daniel Patrick Pereira, Celso Hirata and Simin Nadjm-Tehrani. **A STAMP-based ontology approach to support safety and security analyses**. Journal of Information Security and Applications. Volume 47, August 2019, Pages 302-319. https://doi.org/10.1016/j.jisa.2019.05.014.
- Young, W.; Leveson, N. G., 2014. **An integrated approach to safety and security based on systems theory**. Commun. ACM 57, 2, 31-35. 10.1145/2556938.
- **INCOSE Systems Engineering Handbook** v. 4, International Council on Systems Engineering, 2015.
- **Airworthiness Security Process Specification**. Radio Technical Commission for Aeronautics (RTCA), ED-202A / DO-326A, 2014.

Thank you

Dr. Daniel Patrick Pereira

Cyber security architect for Commercial and Military aircrafts

Airbus Defence & Space

https://www.linkedin.com/in/danielpatrickpereira