Application of STPA-Sec in Military Systems

Amanda Iriarte Quilici

Gabriel Luis de Oliveira

6.9.2022

AGENDA

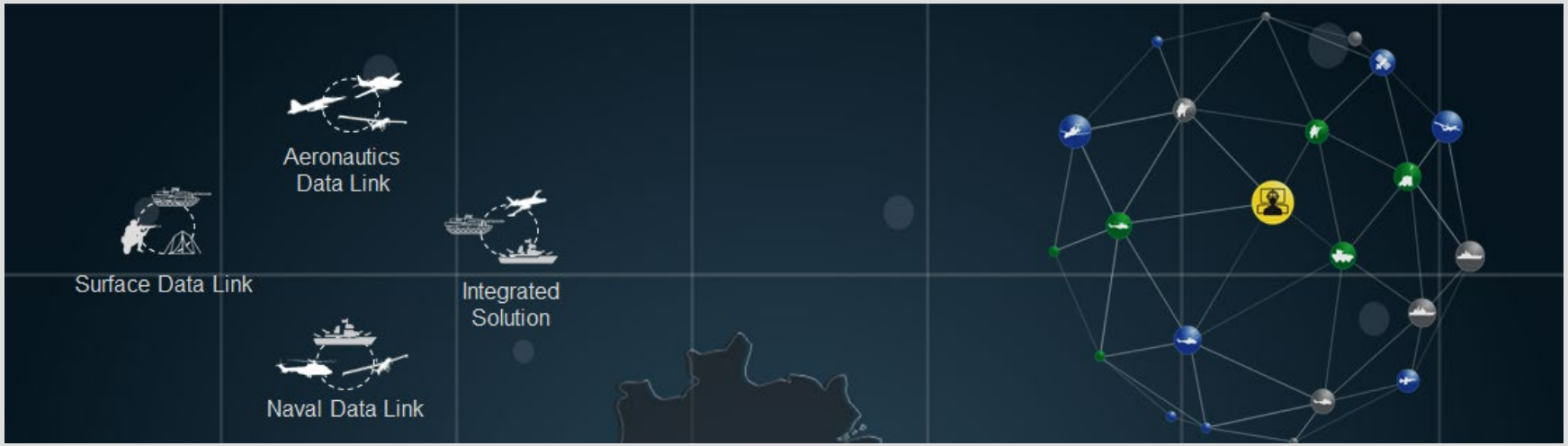
- **Introduction**
  - Our company
  - Data Link System
- **Development**
  - Roles inside the Analysis
  - Losses, Hazards, Control Structure, UCAs, causal scenarios
- **Results**
- **Conclusions and next steps**

OUR COMPANY

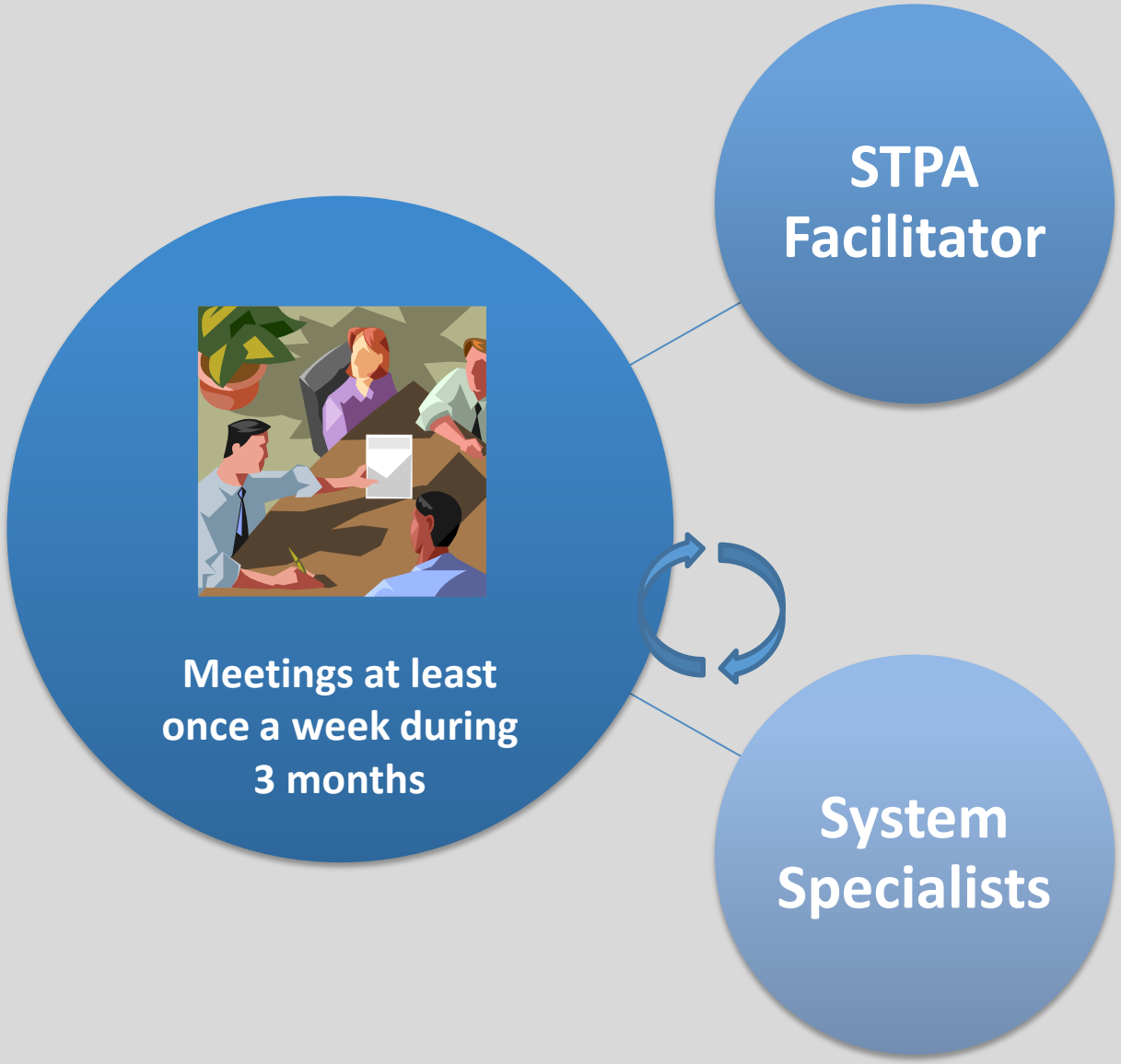

SERVICES
AVIONICS
UAVs
TRAINING AND SIMULATIION
ÆL SISTEMAS
SOLUTIONS FOR ARMORED VEHICLES
SPACE SYSTEMS
TACTICAL COMMUNICATION
ELECTRONIC WARFARE
ELECTRO-OPTICS

Introduction - Data Link System

- The Data Link is a tactical communication system that interacts with ground, air, command and control (C2) and aircraft pilots
- **Objective:** Keep the system resilient to any kind of security attack
  - Output of the Analysis: Generate good design recommendations in order to have a robust requirements basis
- As the system is confidential the presented results are generic and illustrative



Development – Roles during the STPA procedure



- A Systems Engineer who knows the method

- Software Engineers
- Hardware Engineers
- Systems Engineers
- Security Engineers
- Pilots

Development – Defining the purpose of the Analysis

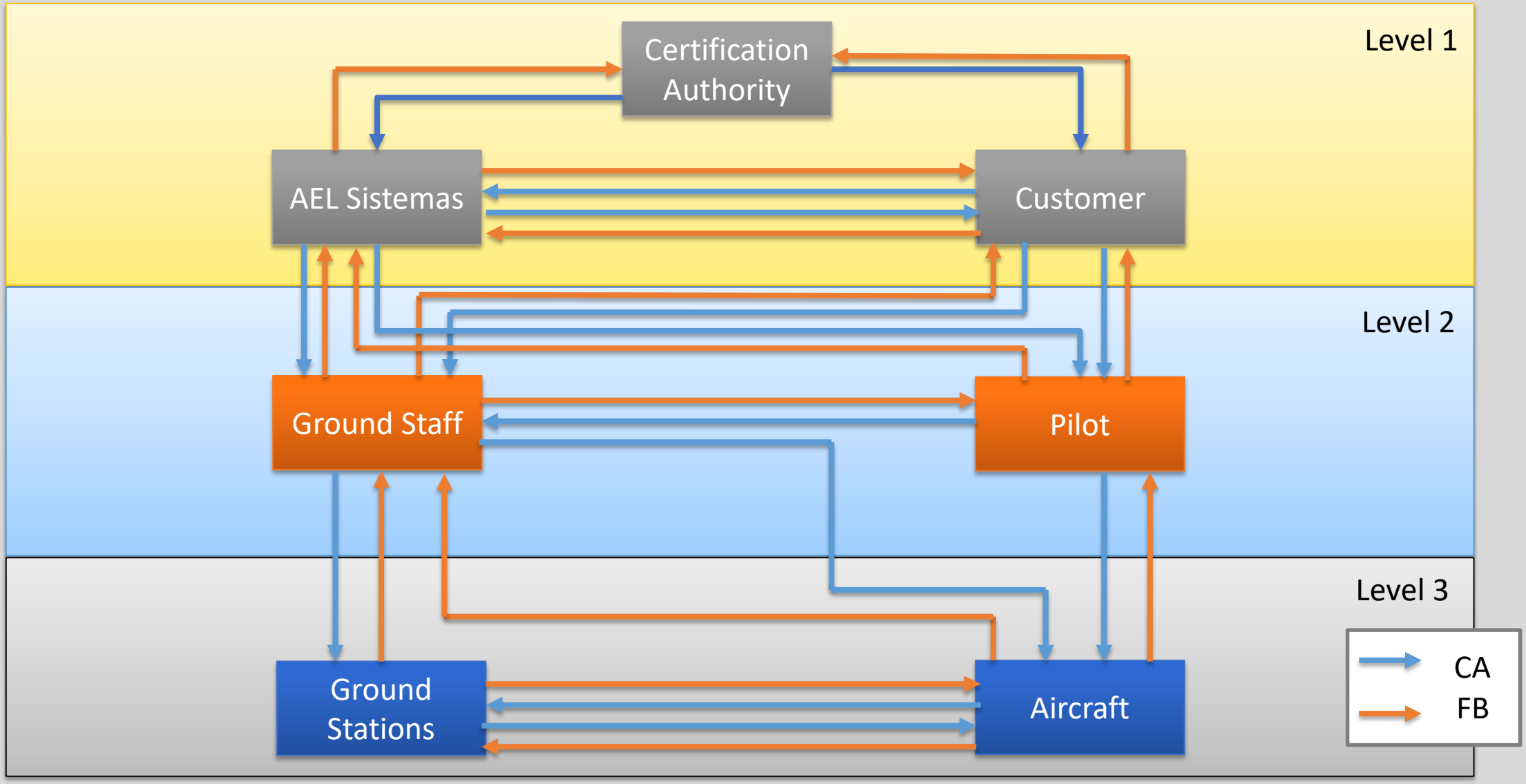
- Identify **Losses**
- Identify system-level **Hazards**

ID	STPA-Sec Loss*
L01	Loss of integrity of communication
L02	…
L03	…
L0N	…

ID	STPA-Sec Hazards*	Losses
H-1	Lack of ability of aircraft to receive and transmit the proper data	…
H-2	Enter data with unauthorized modification	L01
H-N	…	…

*Illustrative examples

Development – Modeling the Control Structure



Simplified/Illustrative Control Structure

Development – UCA illustrative example

ID	Controller	Control Action	Controlled Process	UCA ID	Hazard	Provide	UCA ID	Hazard	Not Provide	UCA ID	Hazard	Too Late, Too Early, Wrong order
A1	Maintenance Operator	Maintenance Operator updates load data into the Aircraft	Aircraft A	1	H1 H2 H3	Maintenance Operator updates load data when it is tampered	2	H1 H3	The Maintenance Operator does not update aircraft load data	3	H1	Maintenance Operator updates load data using a wrong order of the interface setup

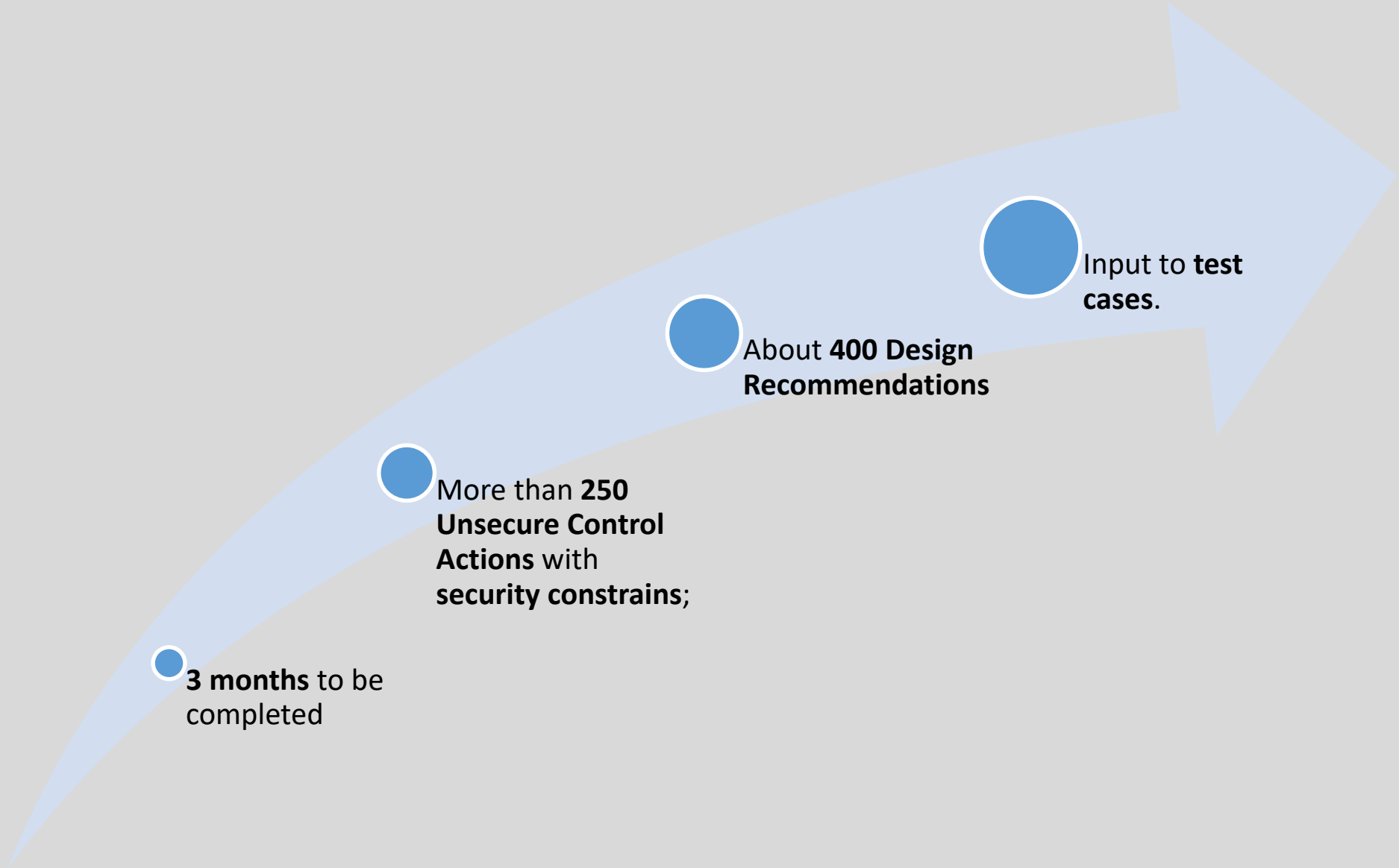
	Scenarios	Causal Factors
1	Operator believes the data has integrity and follow the procedures to update data into the aircraft	An attacker modified the load data in the maintenance computer considering it has no protection

Security Design recommendation 1

- Confidentiality protection to prevent acquisition of information by attackers
- Integrity protection to detect manipulation of data by attackers
- Require identification and authentication to use the maintenance computer

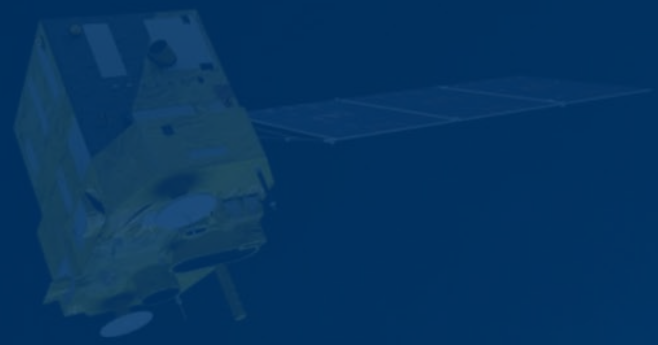
Sec_ Rec_ 01	- The Data Link System maintenance computer shall perform an integrity check of the update data - …

Results



Conclusions and next steps

- **Worthwhile effort, producing a robust requirements basis in a short period of time**
- **A complex system became easier to be analyzed**
- **Recommendation to execute the STPA in the next security analysis within the company**
- **Increase of internal interest**
- **Next Steps:**
  - Integrate it with the MBSE
  - Continue disseminating the STAMP/STPA within the company



Thank you!

ael.com.br

Amanda Iriarte Quilici
Systems Engineer Coordinator
AEL SISTEMAS
aquilici@ael.com.br

Gabriel Luis de Oliveira
Systems Engineer
AEL SISTEMAS
goliveira@ael.com.br