34th Annual INCOSE international symposium

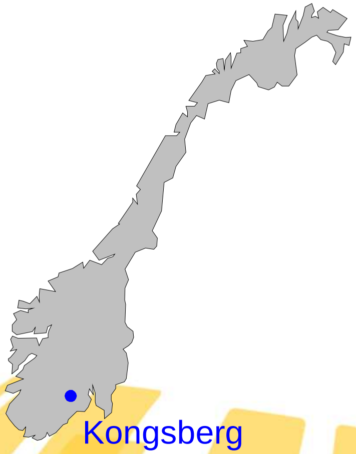
hybrid event

Dublin, Ireland
July 2 - 6, 2024

A Proposal for Model-Based Systems Engineering Method for Creating Secure Cyber-Physical Systems

Martin Larsen, Satya Kokkula, Gerrit Muller
University of South-Eastern Norway

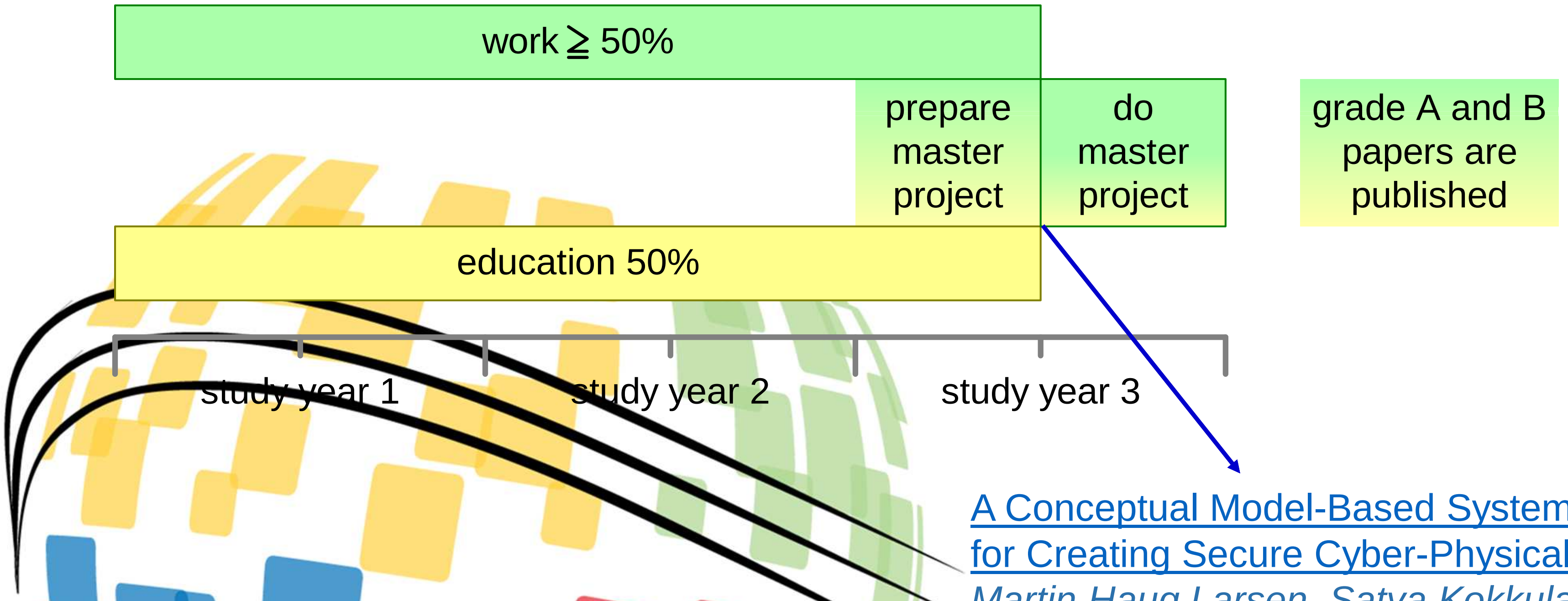
Technology park Kongsberg



Research Model Master Students Systems Engineering in Kongsberg, Norway

students know:
+ domain
+ SE methods
and techniques

students:
+ apply
+ reflect
+ evaluate



[A Conceptual Model-Based Systems Engineering Method for Creating Secure Cyber-Physical Systems](), *Martin Haug Larsen, Satya Kokkula and Gerrit Muller*; CSER 2022 online conference

Context

- Jotron AS
- Air Traffic Control (ATC) technology company in Norway
- Approximately 399 employees

Background

- The aviation industry is being increasingly exposed to rising levels of cyber security risk
- Cyber security has never been more important
- Security risks are identified late in the system development life-cycle
- INCOSE Systems Engineering Vision 2035 included cyber security as one of the ten key system characteristics expected by stakeholders (INCOSE, 2021)

Research Questions

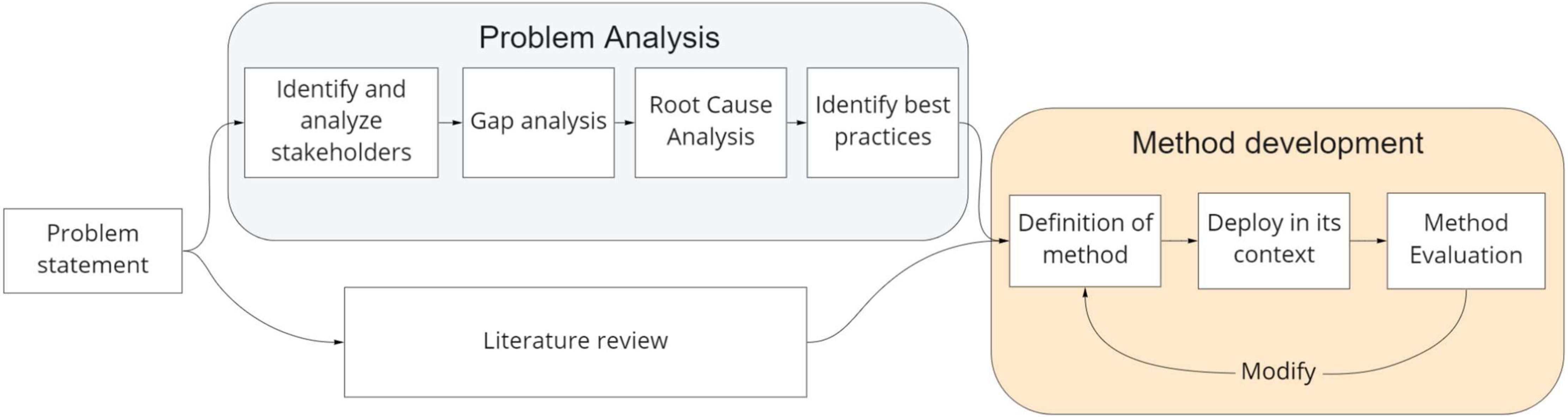
RQ1

How can cyber security risks be **mitigated early** in the system development process?

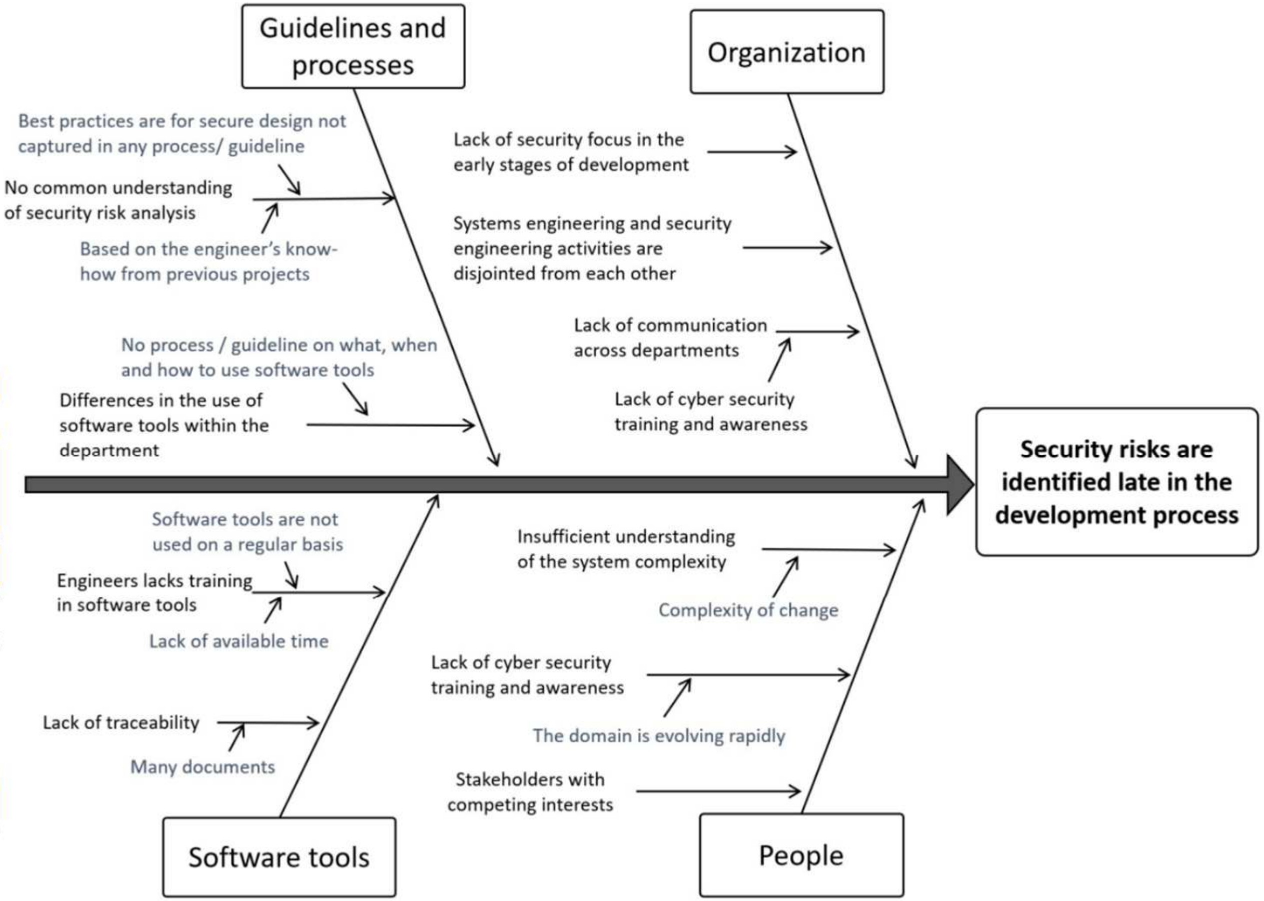
RQ2

How can cyber security concepts **fit into** the systems engineering process for increased security?

Research Methodology



Problem Analysis – Root Cause Analysis



Guidelines and processes

Best practices are for secure design not captured in any process/ guideline

No common understanding of security risk analysis

Based on the engineer's know-how from previous projects

No process / guideline on what, when and how to use software tools

Differences in the use of software tools within the department

Organization

Lack of security focus in the early stages of development

Systems engineering and security engineering activities are disjointed from each other

Lack of communication across departments

Lack of cyber security training and awareness

Security risks are identified late in the development process

Software tools are not used on a regular basis

Engineers lacks training in software tools

Lack of available time

Lack of traceability

Many documents

Software tools

Insufficient understanding of the system complexity

Complexity of change

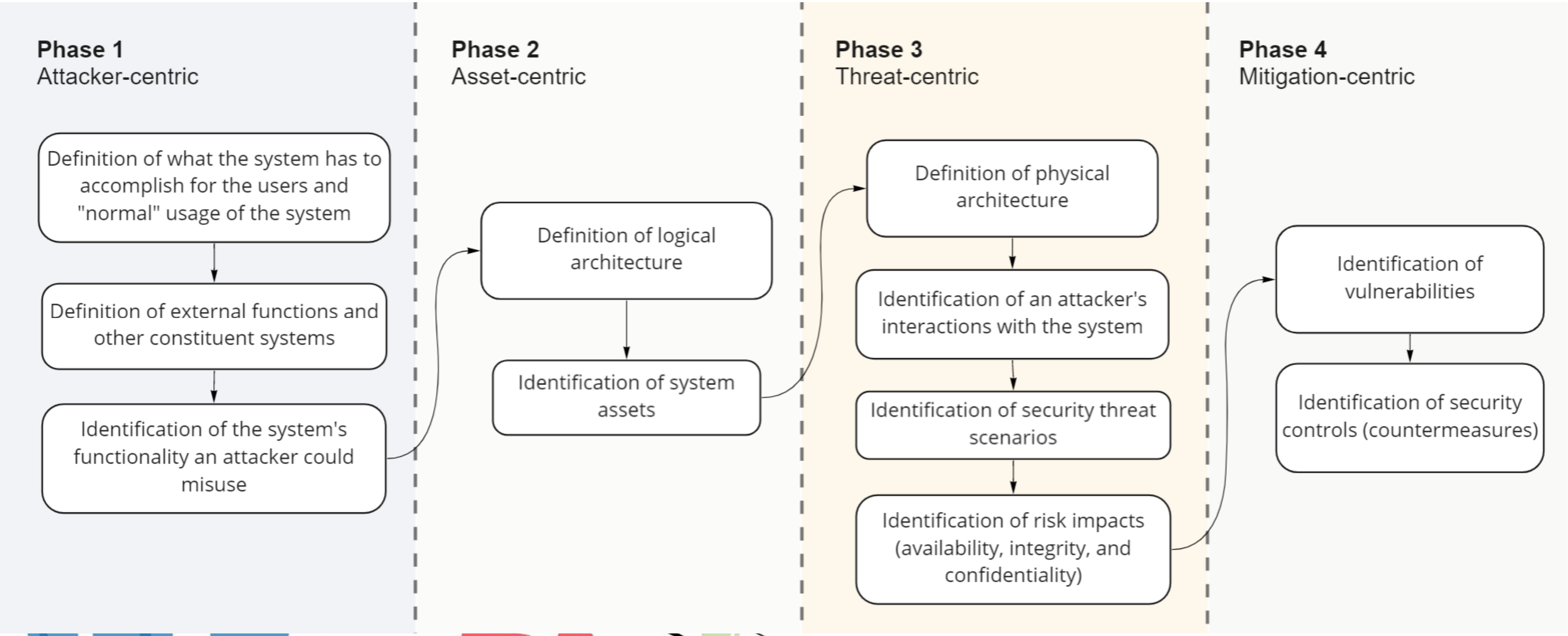
Lack of cyber security training and awareness

The domain is evolving rapidly

Stakeholders with competing interests

People

MBSE Security Analysis Method



Phase 1
Attacker-centric

Definition of what the system has to accomplish for the users and "normal" usage of the system

Definition of external functions and other constituent systems

Identification of the system's functionality an attacker could misuse

Phase 2
Asset-centric

Definition of logical architecture

Identification of system assets

Phase 3
Threat-centric

Definition of physical architecture

Identification of an attacker's interactions with the system

Identification of security threat scenarios

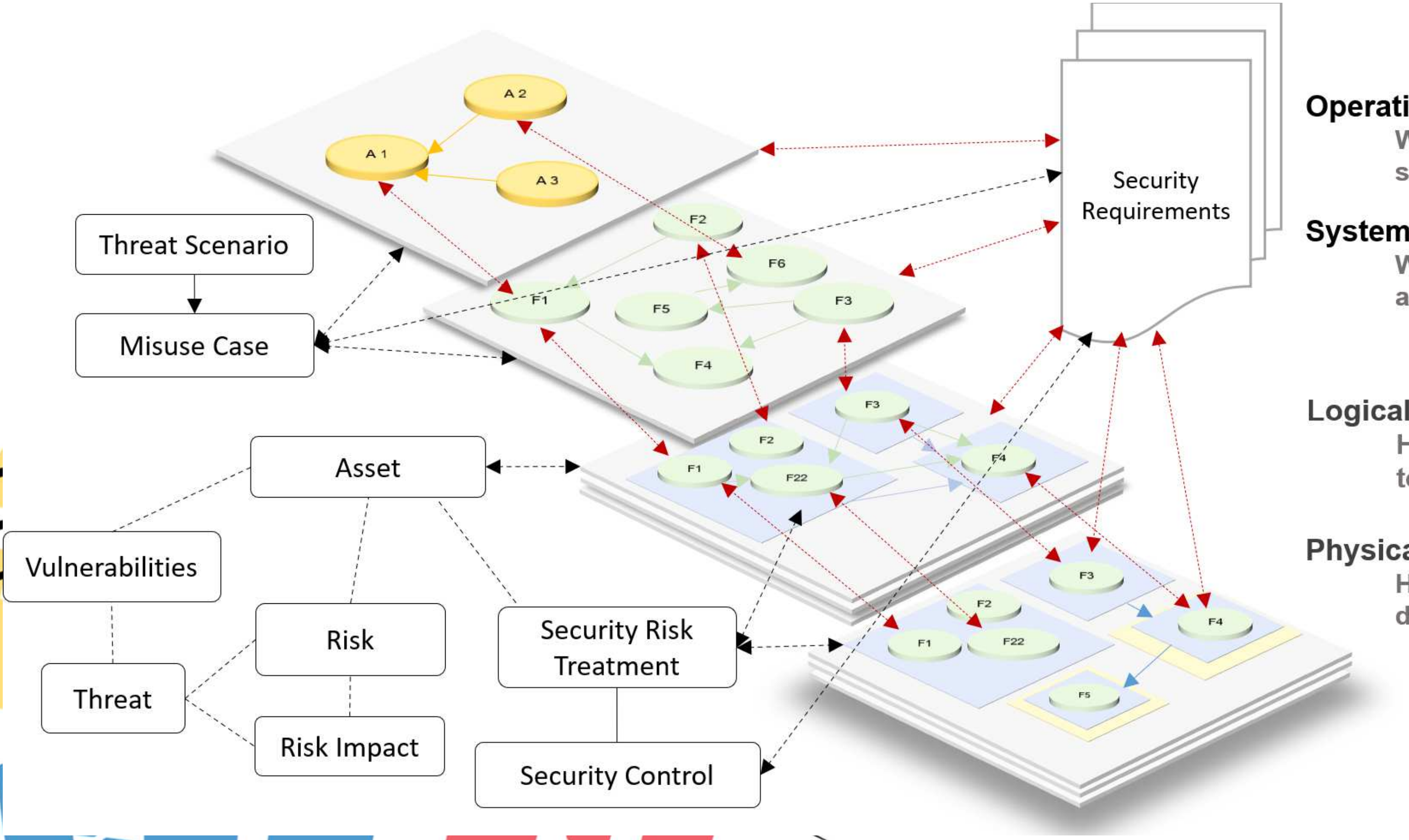
Identification of risk impacts (availability, integrity, and confidentiality)

Phase 4
Mitigation-centric

Identification of vulnerabilities

Identification of security controls (countermeasures)

MBSE Security Analysis Method



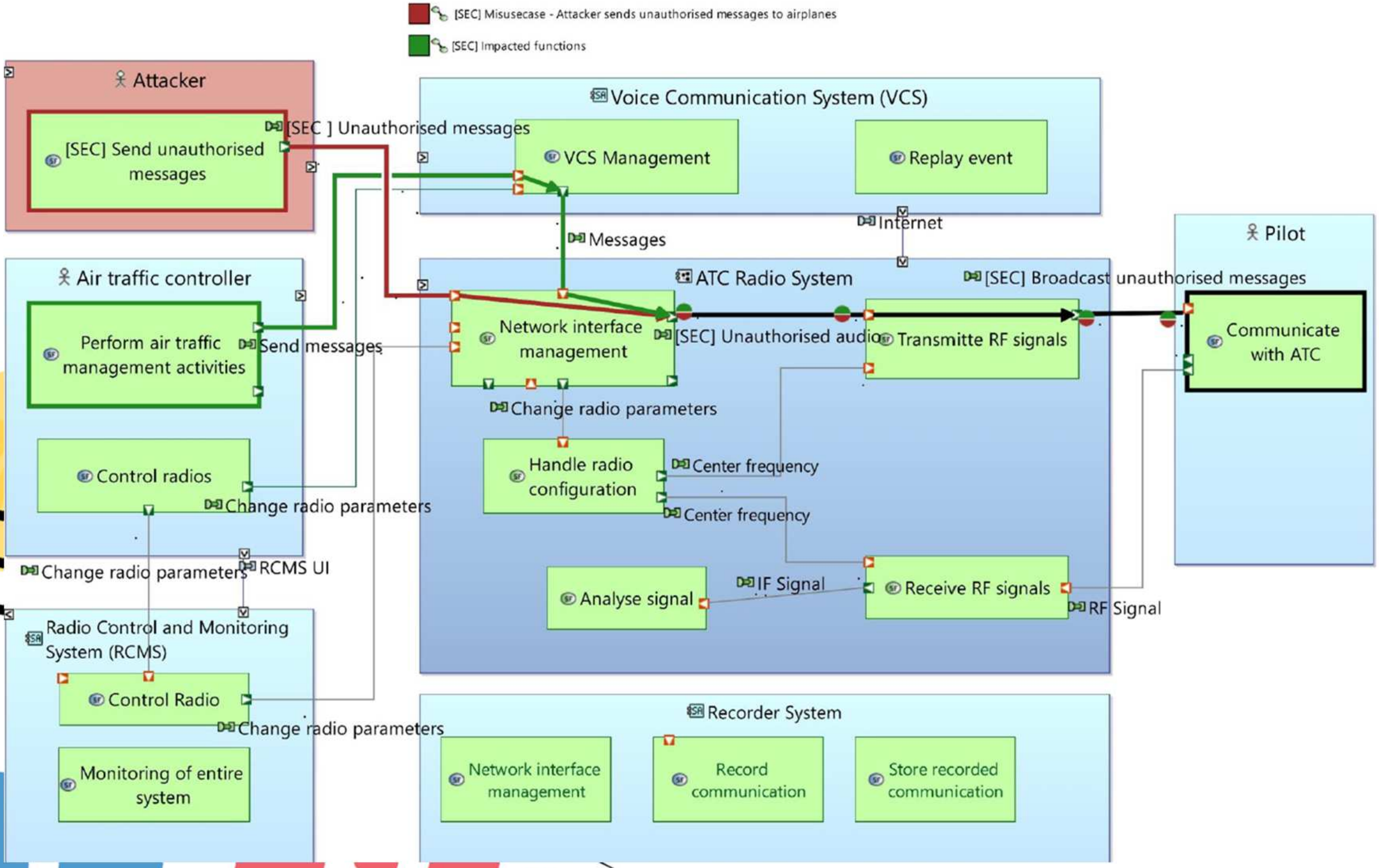
Operational Analysis
What the users of the system need to accomplish

System Analysis
What the system has to accomplish for the users

Logical Architecture
How the system will work to fulfill expectations

Physical Architecture
How the system will be developed and built

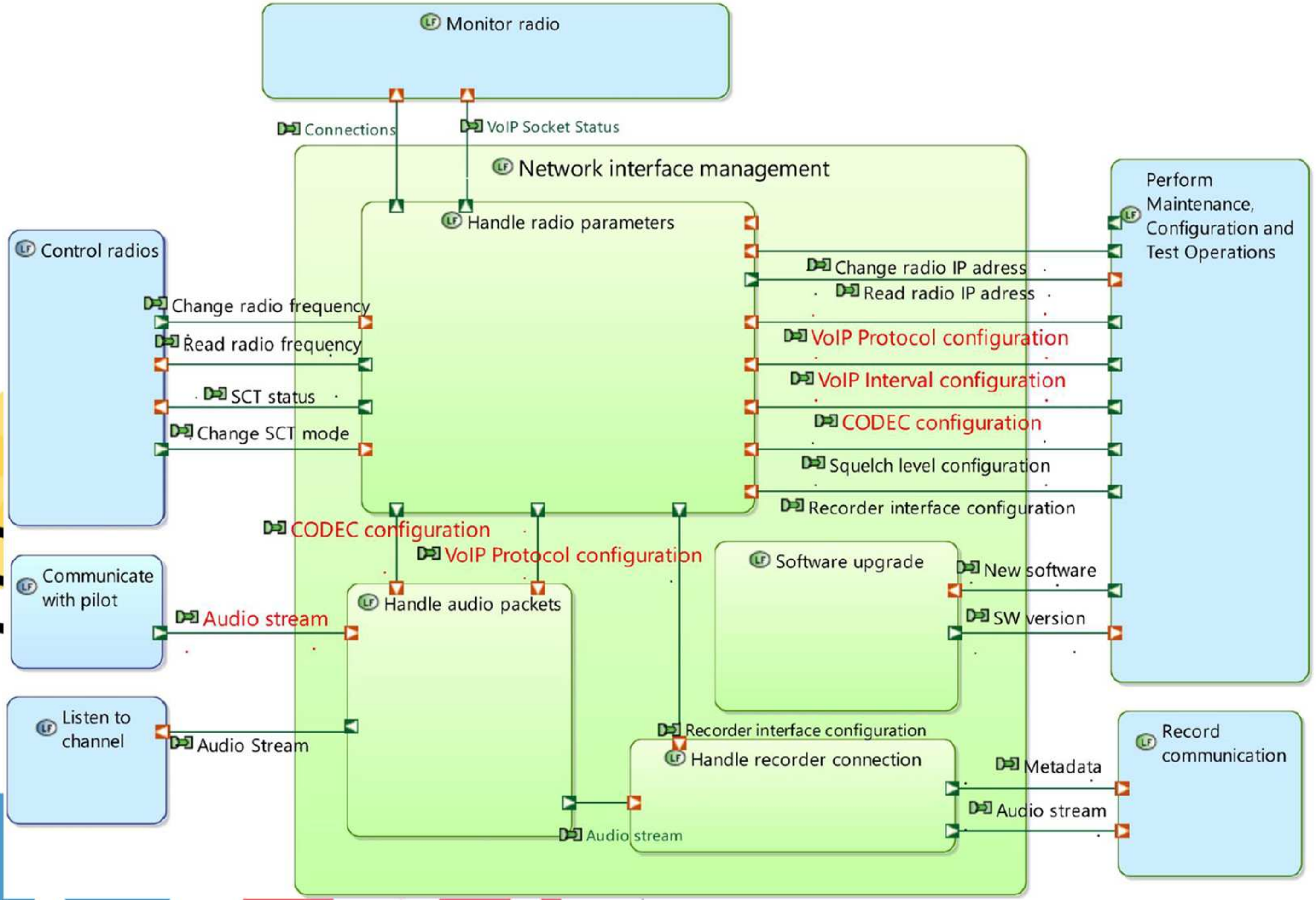
Phase 1 – Attacker-centric



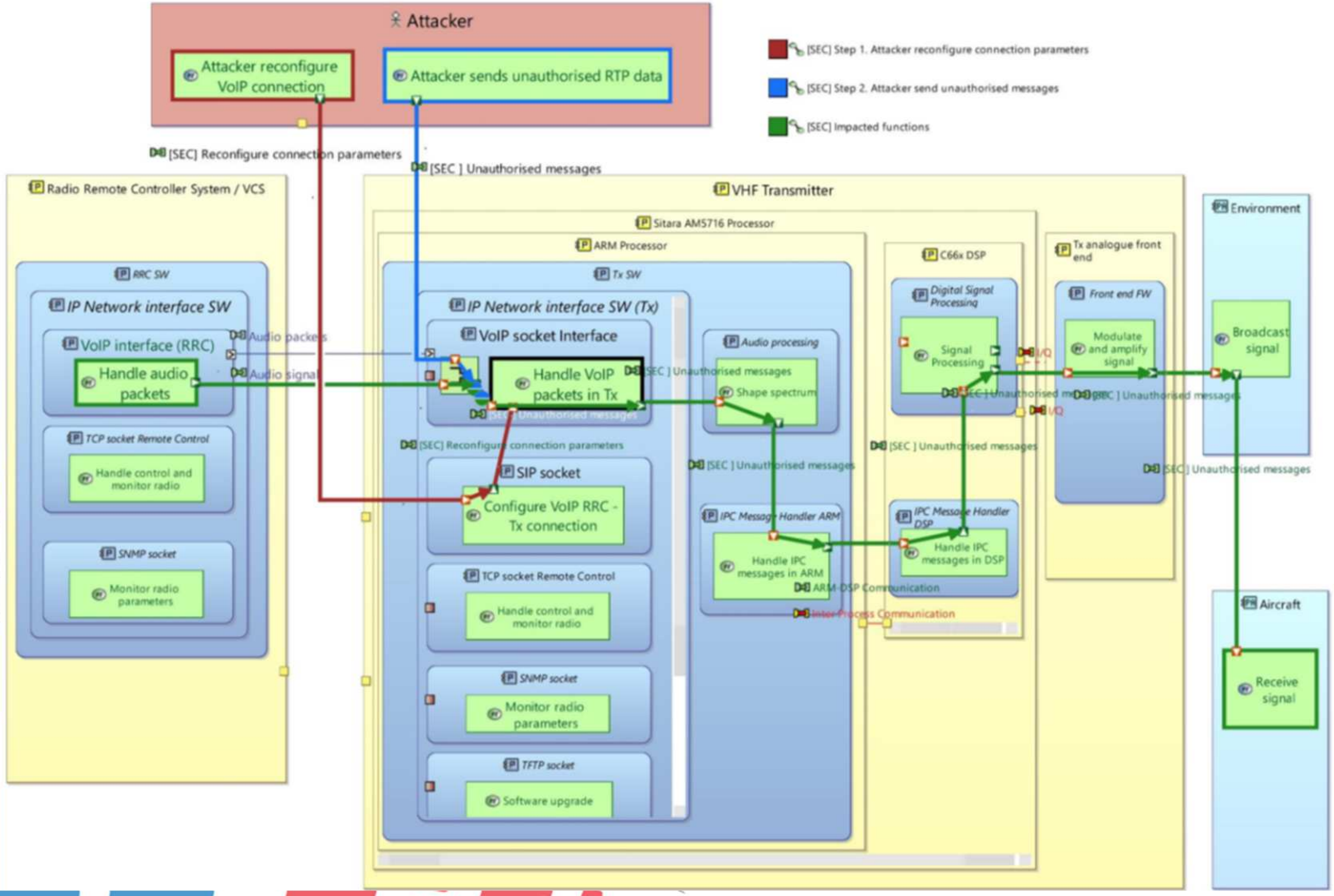
🟥 [SEC] Misusecase - Attacker sends unauthorised messages to airplanes

🟩 [SEC] Impacted functions

Phase 2 – Asset-centric

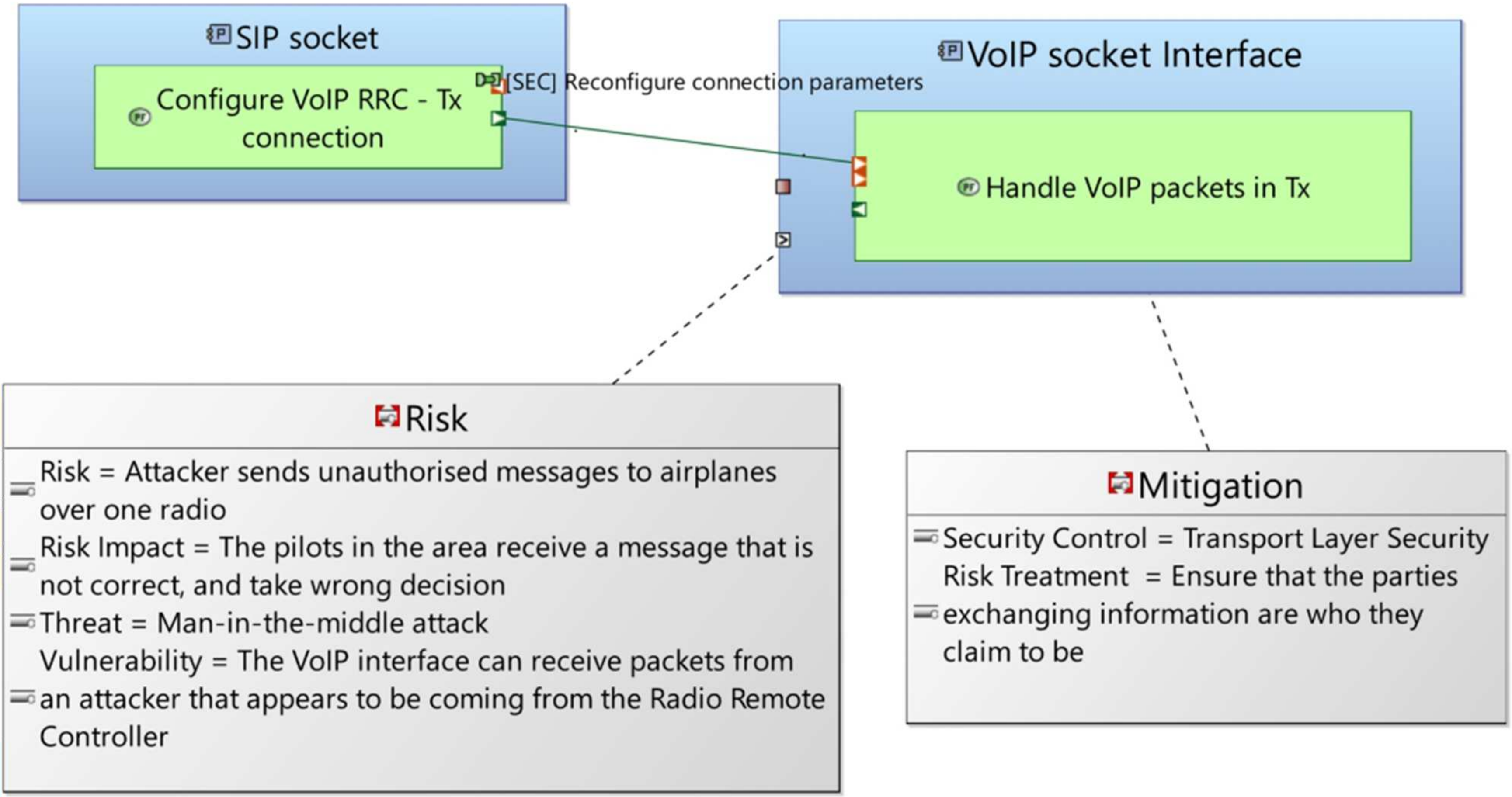


Phase 3 – Threat-centric



Attacker
Attacker reconfigure VoIP connection
Attacker sends unauthorised RTP data
[SEC] Step 1. Attacker reconfigure connection parameters
[SEC] Step 2. Attacker send unauthorised messages
[SEC] Impacted functions
[SEC] Reconfigure connection parameters
[SEC] Unauthorised messages
Radio Remote Controller System / VCS
RRC SW
IP Network interface SW
VoIP interface (RRC)
Handle audio packets
Audio packets
Audio signal
TCP socket Remote Control
Handle control and monitor radio
SNMP socket
Monitor radio parameters
VHF Transmitter
Sitara AM5716 Processor
ARM Processor
Tx SW
IP Network interface SW (Tx)
VoIP socket Interface
Handle VoIP packets in Tx
[SEC] Unauthorised messages
[SEC] Reconfigure connection parameters
SIP socket
Configure VoIP RRC - Tx connection
TCP socket Remote Control
Handle control and monitor radio
SNMP socket
Monitor radio parameters
TFTP socket
Software upgrade
Audio processing
Shape spectrum
[SEC] Unauthorised messages
IPC Message Handler ARM
Handle IPC messages in ARM
ARM-DSP Communication
Inter Process Communication
C66x DSP
Digital Signal Processing
Signal Processing
I/Q
[SEC] Unauthorised messages
IPC Message Handler DSP
Handle IPC messages in DSP
Tx analogue front end
Front end FW
Modulate and amplify signal
Environment
Broadcast signal
Aircraft
Receive signal

Phase 4 – Mitigation-centric


SIP socket
Configure VoIP RRC - Tx connection
[SEC] Reconfigure connection parameters
VoIP socket Interface
Handle VoIP packets in Tx

Risk

Risk = Attacker sends unauthorised messages to airplanes over one radio

Risk Impact = The pilots in the area receive a message that is not correct, and take wrong decision

Threat = Man-in-the-middle attack

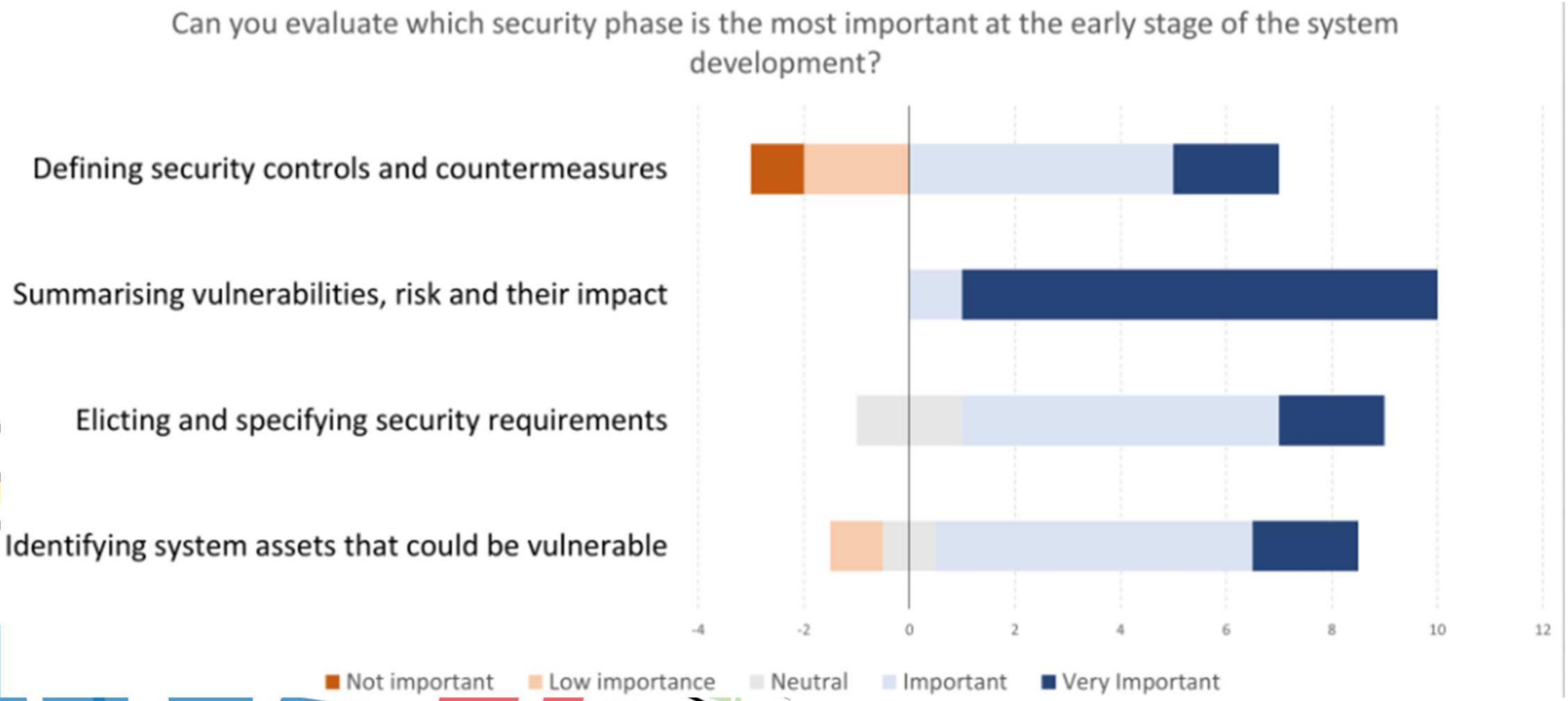
Vulnerability = The VoIP interface can receive packets from an attacker that appears to be coming from the Radio Remote Controller

Mitigation

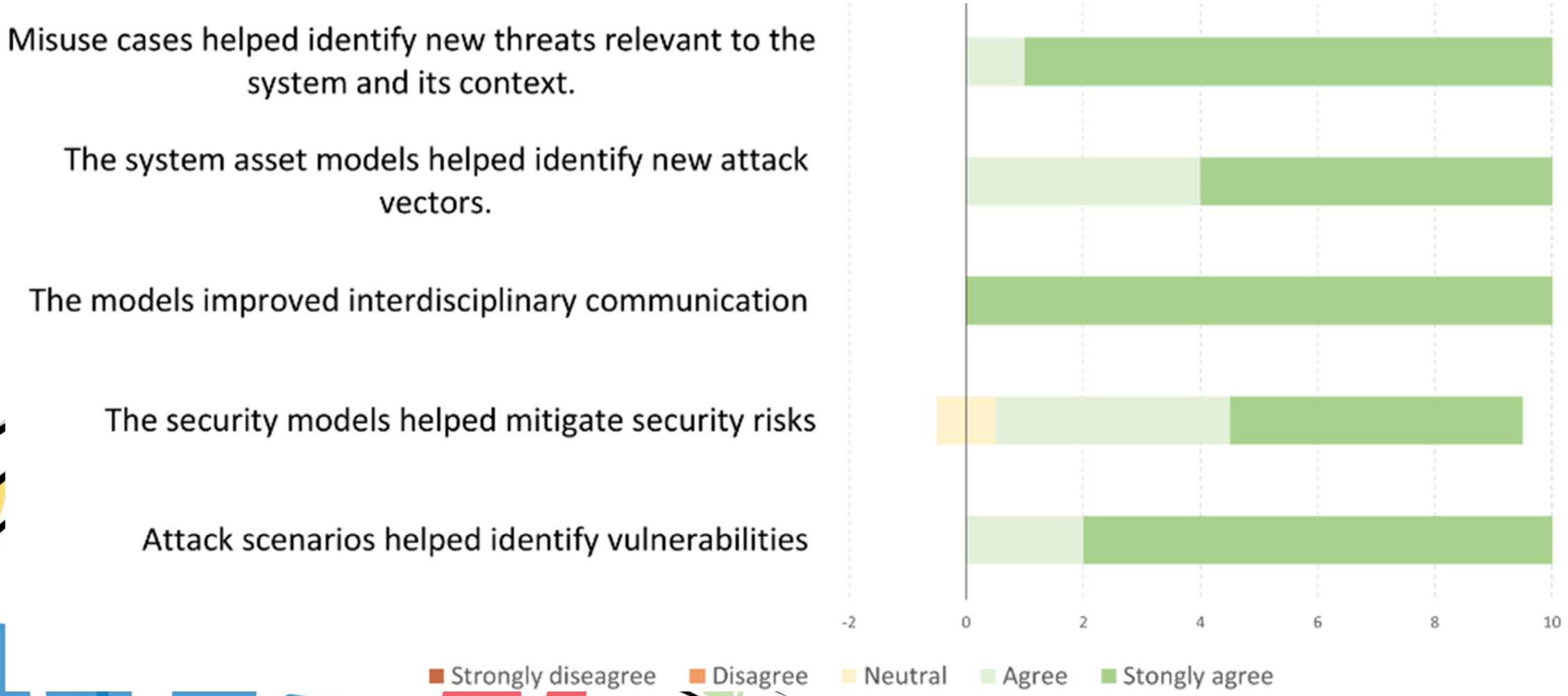
Security Control = Transport Layer Security

Risk Treatment = Ensure that the parties exchanging information are who they claim to be

Method Evaluation



Method Evaluation



Discussion

- How can cyber security risks be mitigated early in the system development process?
- How can cyber security concepts fit into the systems engineering process for increased security?
- Taking advantage of MBSE
- Different approach similar results?
- **Engineers identify threats and vulnerabilities, not the method**
- Limitations to this researchs validity

Conclusion

- Early security risk identification
- Incorporate mitigation strategies into the system design
- Improved interdisciplinary communication
- Potential for early identification of security risks using models

Future Research

- Future versions of the proposed model-based method
- Add more academic contributions to the literature
- Larger sample size
- Compare the proposed method to other methods

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS