Empirical Studies of Methods for Safety and Security Co-analysis of Autonomous Boat

Erik Nilsen Torkildson, Jingyue Li, Stig Ole Johnsen
Norwegian University of Science and Technology (NTNU)

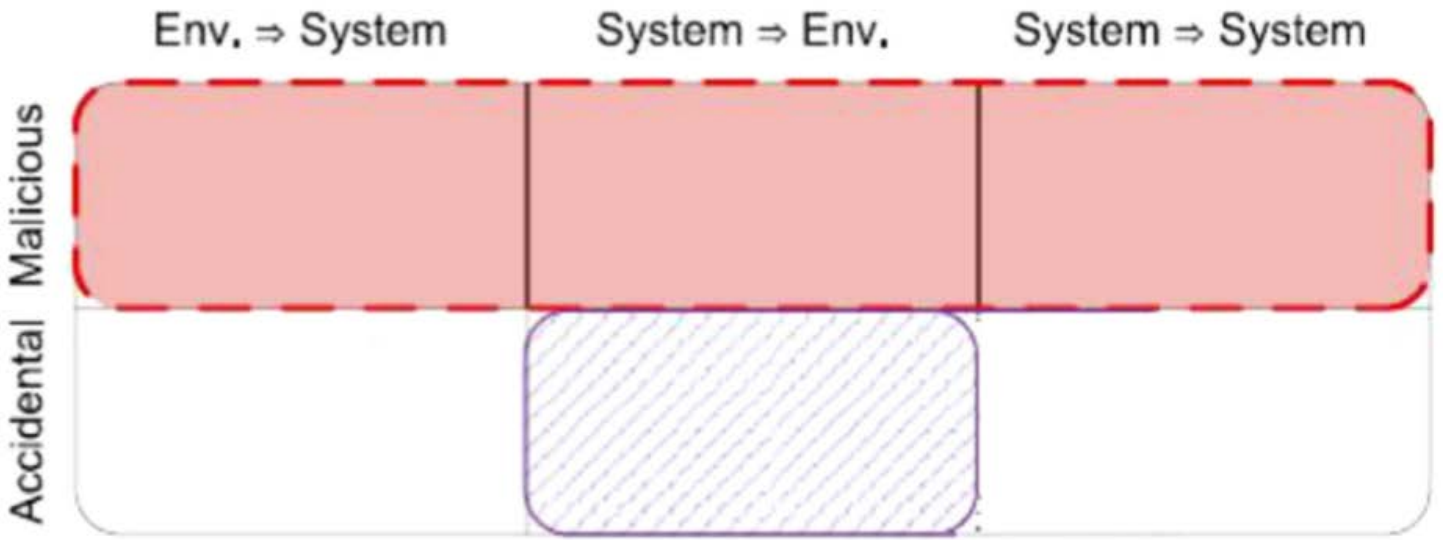
Jon Arne Glomsrud
DNVGL

Outline

- State of the art
- Research questions
- Research design
- Results
- Conclusions

Safety vs. Security

- Safety: accidental harm
- Security: intentional harm



[1]

Safety and Security Interactions

- **Conditional dependency:** Safety level is dependent on security level.
- **Mutual reinforcement**: Satisfaction of safety requirements contributes to security, or vice-versa.
- **Antagonism**: When considered jointly, safety and security requirements lead to conflicting situations.
- **Independency:** No interaction.

Safety and Security Co-analysis

- Many methods have been proposed
- Can be summarized into three categories [2]
  - Generic approach
  - Model-based graphical methods
  - Model-based non-graphic methods
- Lack of empirical comparisons of the methods

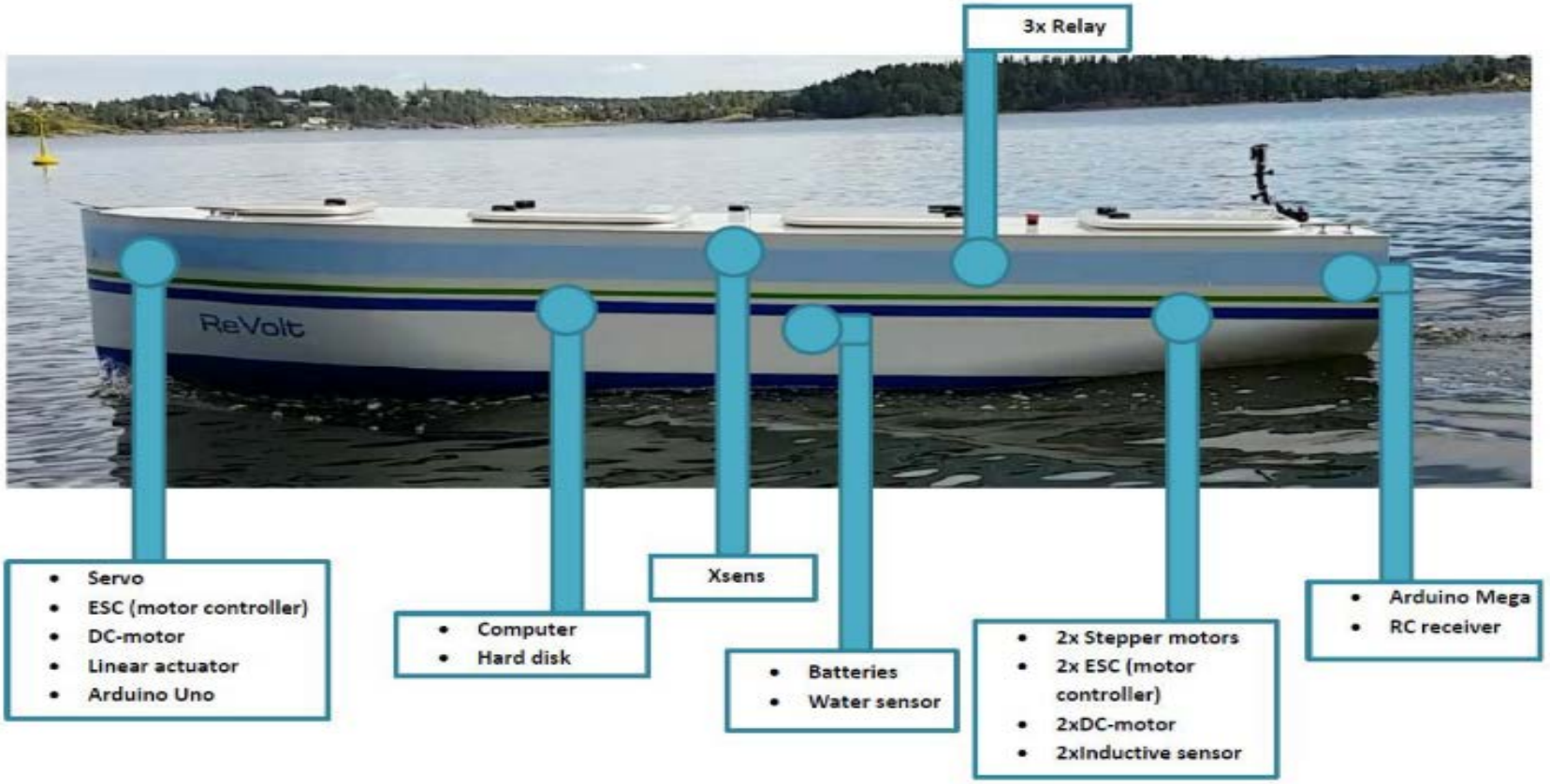
Our Research Motivation

- Choose one “safety and security co-analysis method” in each category

- Empirically compare
  - Their efficiency
  - Hazards they can identify
  - Their applicability

- Focus on CPS, especially autonomous system

Our Autonomous Boat - Revolt



Not pure autonomous yet, but a remotely operated dynamically positioned boat

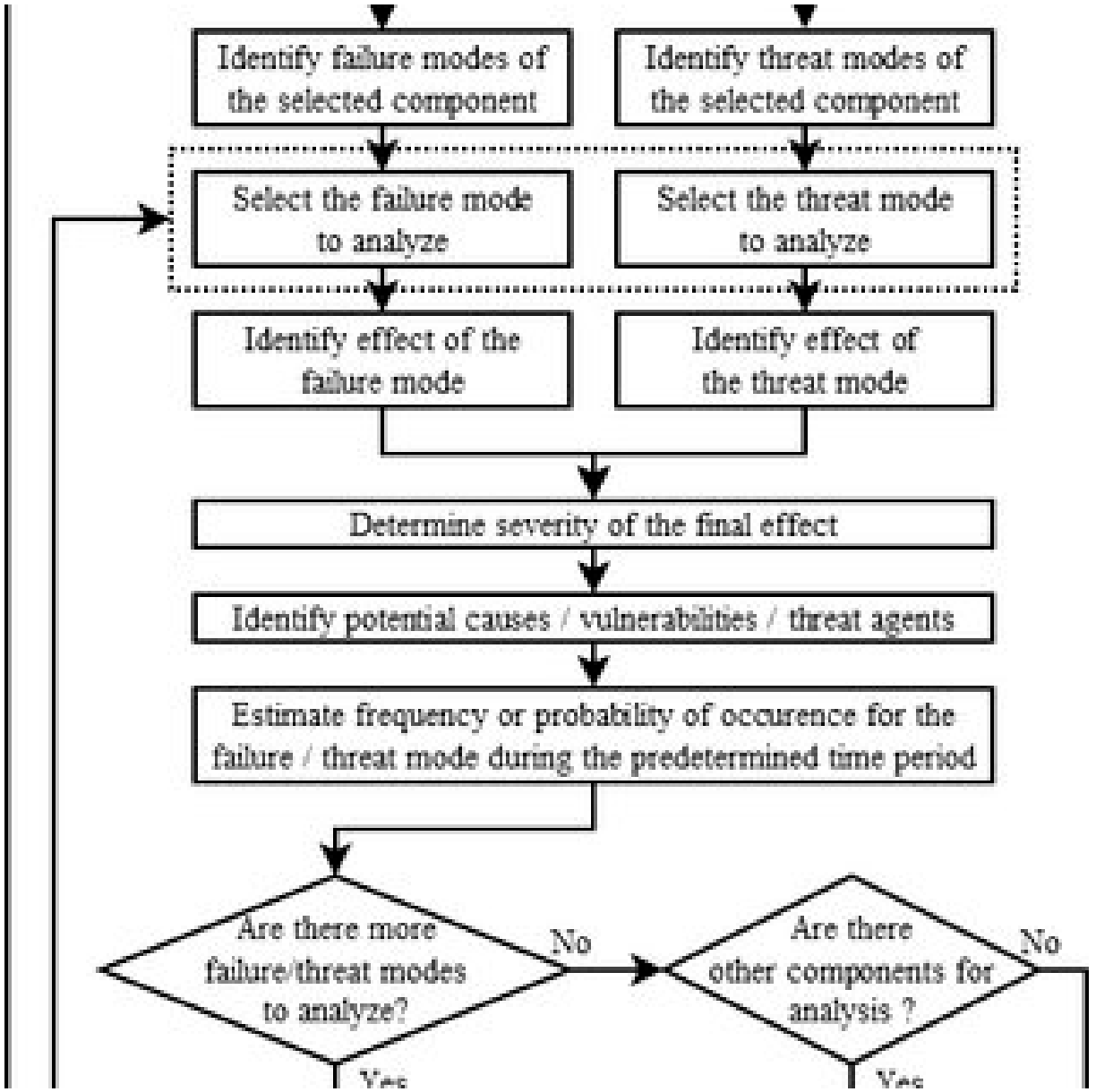
We Compared Three Methods

- **FMVEA** (Failure Mode, Vulnerabilities and Effect Analysis)
- **CHASSIS** (Combined Harm Assessment of Safety and Security for Information Systems)
- **STPA (**System Theoretic Process Analysis) plus **STPA-Sec**

FMVEA

STRIDE threat mode

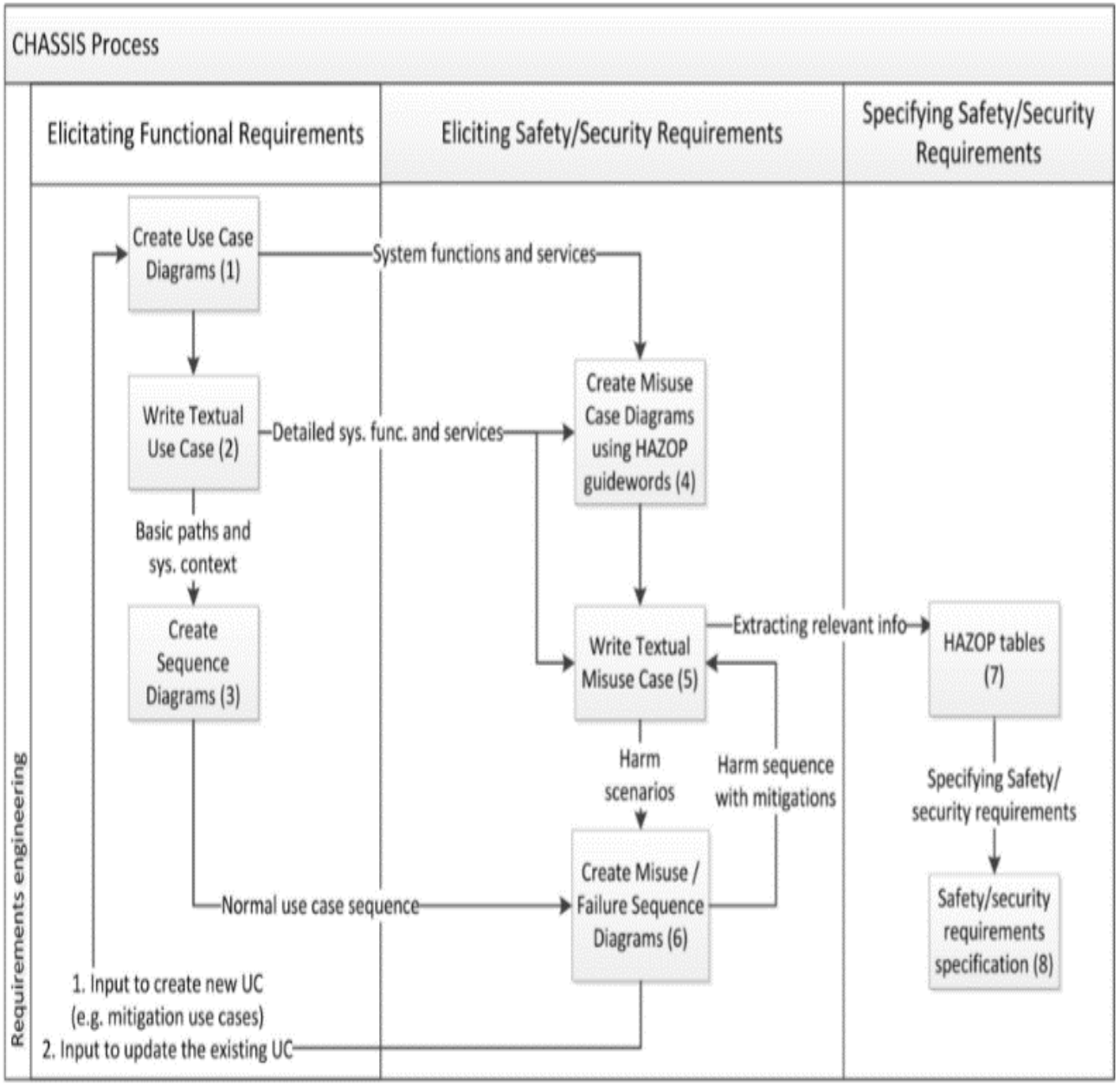
- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege



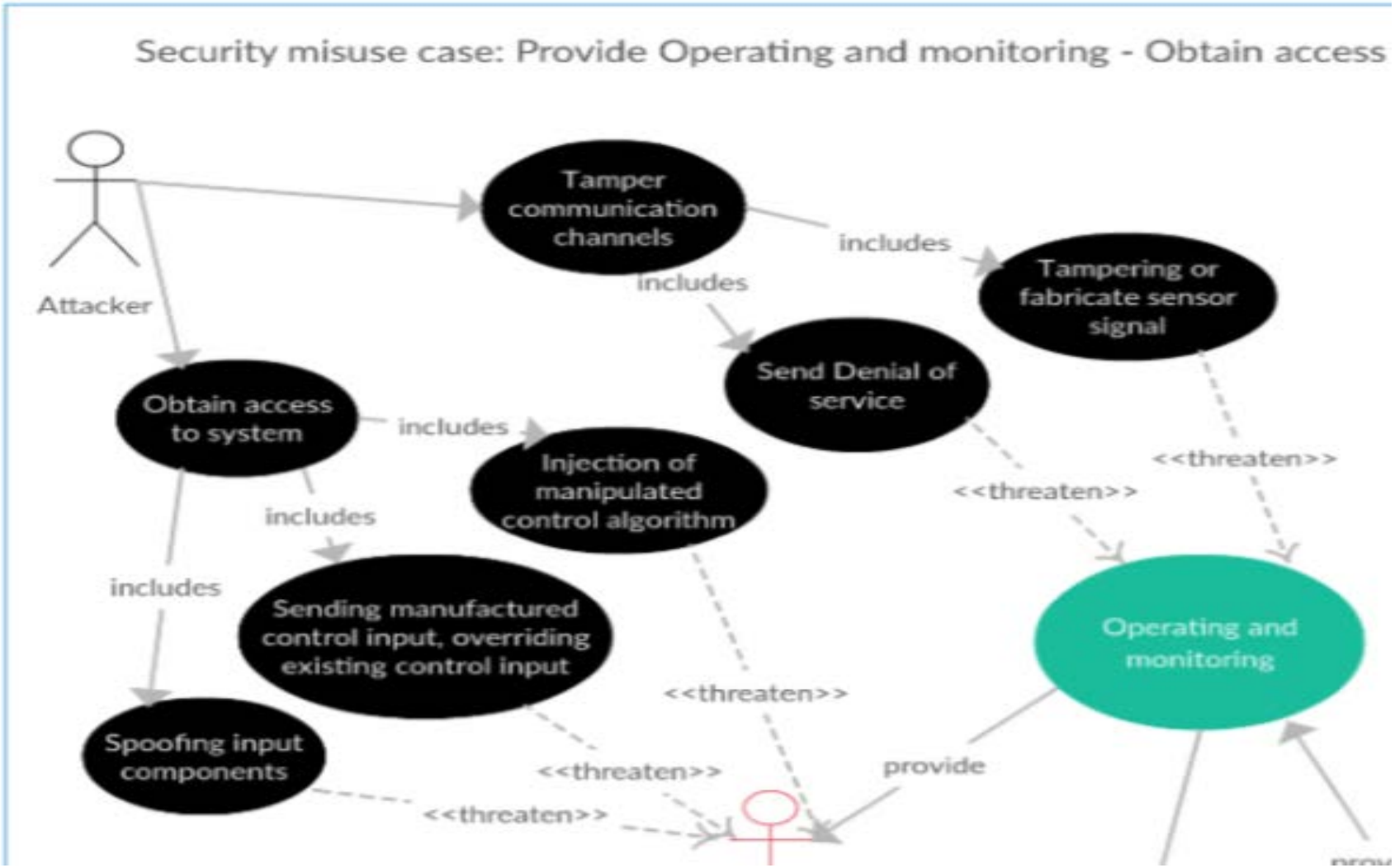
FMVEA Result Example

ID	component / element	Vulnerability/ Failure Cause	Threat Mode/ Failure Mode	Threat Effect/ Failure Effect	System Status	System Effect	Severity	System Susceptibility	Threat Properties	Attack/Failure Probability	Risk
1	WIFI connection	Wireless connection is targeted to jamming	Attacker interrupts connection between operator and Revolt	Revolt is unreachable	Remote operation	Attacker has control over the Revolt's system	Critical:4	4	5	9	36

CHASSIS


CHASSIS Process
Elicitating Functional Requirements
Eliciting Safety/Security Requirements
Specifying Safety/Security Requirements
Requirements engineering
Create Use Case Diagrams (1)
System functions and services
Write Textual Use Case (2)
Detailed sys. func. and services
Create Misuse Case Diagrams using HAZOP guidewords (4)
Basic paths and sys. context
Create Sequence Diagrams (3)
Write Textual Misuse Case (5)
Extracting relevant info
HAZOP tables (7)
Harm scenarios
Harm sequence with mitigations
Specifying Safety/ security requirements
Create Misuse / Failure Sequence Diagrams (6)
Normal use case sequence
Safety/security requirements specification (8)
1. Input to create new UC
(e.g. mitigation use cases)
2. Input to update the existing UC

CHASSIS Result Example



STPA plus STPA-Sec

- Identifying what essential services and functions must be protected or what represents an unacceptable loss.
- Identifying system hazards and constraints.
- Drawing the system control structure to identifying unsafe control actions (UCA).
- Determining the potential causes of the unsafe control actions.
- The potential causes could be security vulnerability and threats.

Unacceptable Loss Example

- Collision with vessels, objects, humans/mammals, structures, grounding
- Fire or explosion
- Foundering (sinking, failing or plunging)
- Loss of cargo
- Loss of mission objectives
- Loss of information

UCA and Potential Causes Example

[UCA15] Not providing CA when a spoofing or jamming attack is occurring		
Scenarios	Causal Factors	Design recommendations / requirements
Spoofing attack is occurring, Man in the middle attack on GSM base station	The system has no proception against spoofing attack	The revolts system must follow security standards for protection against spoofing attacks, this must be implemented on system level

Comparisons of Efforts

- Hard to have direct comparisons of the effort
- Inputs to the methods are very different
  - FMVEA analysis focuses on components
  - CHASSIS analysis focuses on use cases
  - STPA plus STPA-Sec analysis focuses on control actions
- STPA plus STPA-Sec and CHASSIS can be more time-consuming than FMVEA, because more activities are included

Comparisons of Hazards Identified

- **FMVEA**: Single component failure
  - Communication connection is lost

- **CHASSIS**: Operation sequences
  - The operator performs operations on the Revolt before having done security and safety procedures

- **STPA plus STPA-Sec**: Interactions between different components or actors
  - Setting route for shipment and launch position when the shipping dock has not permitting the action, because other ships are dispatching at the same time

Challenges of the Methods

- **FMVEA**
  - Safety and security interactions may be overlooked
- **CHASSIS**
  - Relies more heavily on expert knowledge than other methods
- **STPA plus STPA-Sec**
  - Focuses mainly on vulnerability that can be the casual factors for safety hazards
  - Information leakage or privacy issues can be overlooked

Applicable to Autonomous Systems?

- **Complex and high automation systems**
  - STPA plus STPA-Sec are more applicable
  - More interactions, e.g. in emergency cases, the boat needs to change course and slow down at the same time to avoid collision

- **High level intelligence autonomous systems**
  - “Black box” and “Black code” nature
  - None will work, all need to be adapted

Conclusions

- Empirically evaluated three safety and security co-analysis methods
- Each has its strenghes and weaknesses
- None will work for high level intelligence autonomous systems

References

- [1] Piètre-Cambacédès L, Chaudet C. The SEMA referential framework: avoiding ambiguities in the terms ‘security’ and ‘safety’. Int J Crit Infrastruct Prot 2010;3(2):55–66.
- [2] KRIAA, S., PIETRE-CAMBACEDES, L., BOUISSOU, M. & HALGAND, Y. (2015) A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety, 139, 156-178.