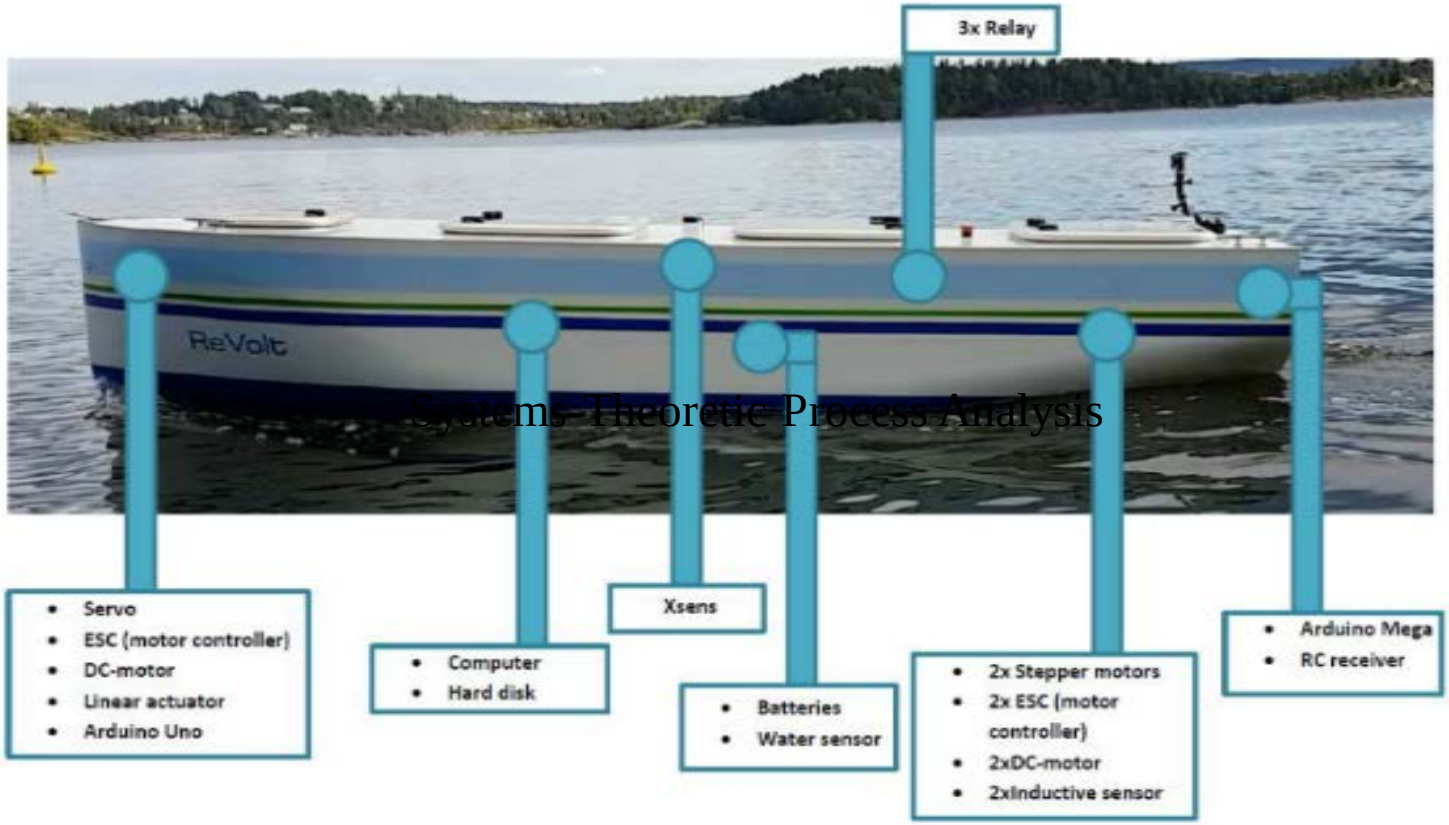
Improving Security and Safety Co-analysis of STPA - Systems-Theoretic Process Analysis

Erik Nilsen Torkildson (Wise Consulting)
Jingyue Li (Norwegian University of Science and Technology)
Stig Ole Johnsen (SINTEF)

Case – Autonomous Boat - Revolt



Safety and Security challenges

- Hackers may hijack and control the autonomous systems remotely, and create mishaps (Fiat recalled 1.4 mill vehicles)
- Drones are vulnerable (an Iranian cyber warfare unit was able to land a US drone based on a spoofing attack modifying global positioning system-GPS data)
- Need to consolidate security and safety analysis – exploring STPA - Systems-Theoretic Process Analysis (Thomas and Leveson)

Safety and Security Interactions

from(Piètre-Cambacédès, 2010)

- **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 ref: KRIAA, S., PIETRE-CAMBACEDES, L., BOUISSOU, M. & HALGAND, Y. (2015)
  - Generic approach (Fault tree)
  - Model-based graphical methods (Cassis)
  - Model-based non-graphic methods (STPA)

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.**

Research questions

- RQ1: What is the security threat modeling analysis that can complement STPA-Sec best and easiest?

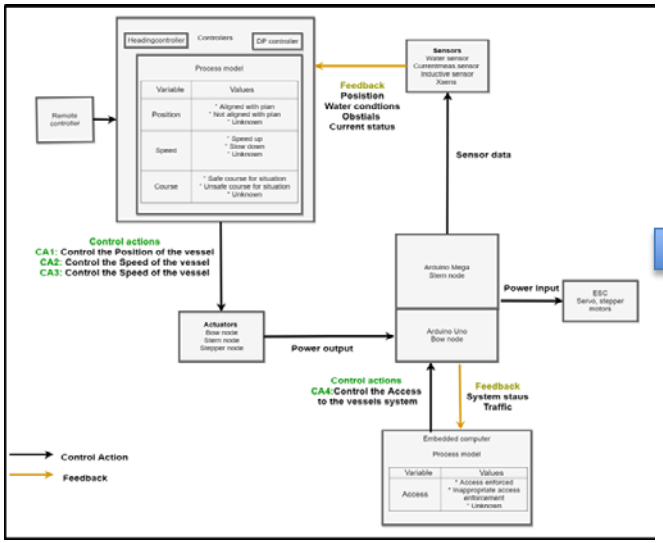
- RQ2: Could we start with security analysis, taking a base in the target assets related risks and consequences, and then consider safety afterward?

RQ1: STPA with threat modeling approaches

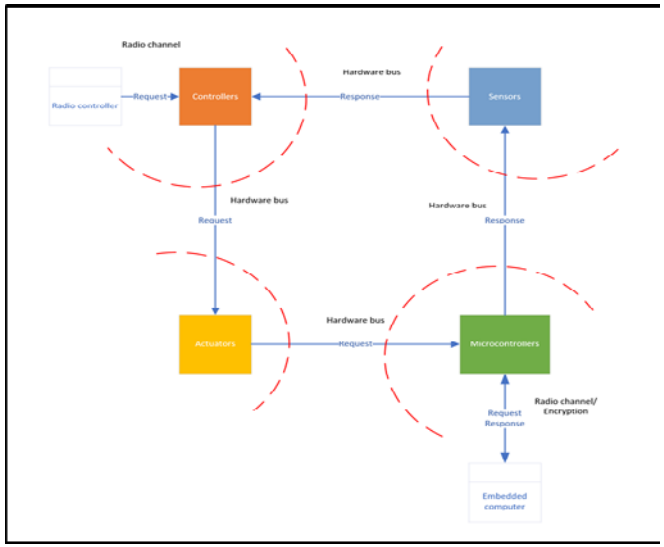
- Misuse cases
  - Helped us discover two more possible security-related threats, which were related to the data flow and encrypting of the communication part of the system.
- Attack tree
  - Helped us discover one more threat, which is due to more in-depth analysis of the possible attacks to tamper the WIFI network.
- Business Process Modelling Notation (BPMN)
  - Helped us discover one more threat, i.e., the possibility to steal information about how the Revolt is maneuvered and what cargo it has.
- Socio-Technical Security modeling language (STS-ml)
  - Did not help us find any new threat.

RQ1: STPA with threat modeling approaches (Cont')

- Data flow diagram



Control structure of the Revolt



Data Flow Diagram Derived

Help identified five more security threats, which are mostly related to the missing encryption between data flow of components.

Results of RQ1

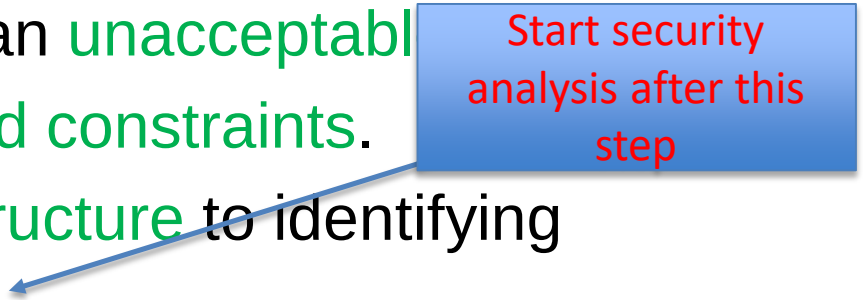
- Combing STPA with threat modeling approaches, such as misuse cases, attach trees, and Business Process Modelling Notation (BPMN), and data flow diagram can find different extra security threats.

- Socio-Technical Security modeling language (STS-ml) did not help

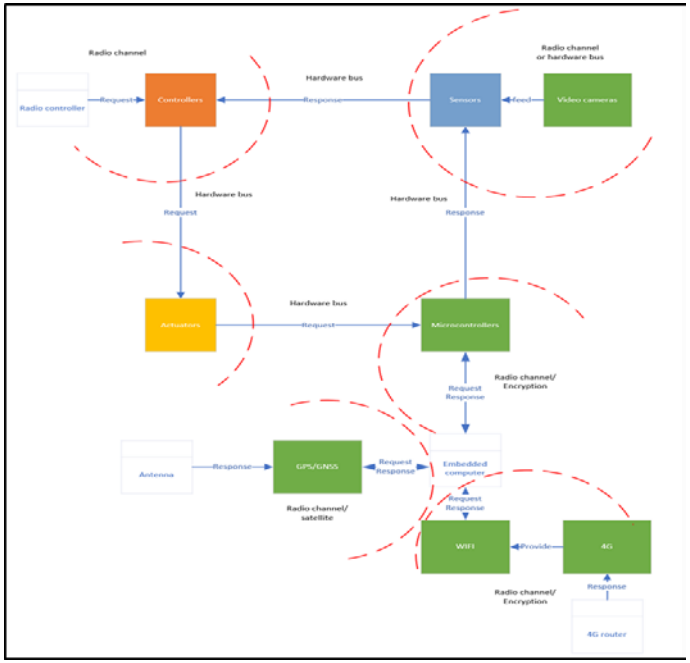
- Data flow diagram is the most easy to use, because the data flow diagram can be easily derived from the control structure created in STPA analysis

RQ2: Move security to early stage of STPA

- Identifying what essential services and functions must be protected or what represents an unacceptabl
- 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.**

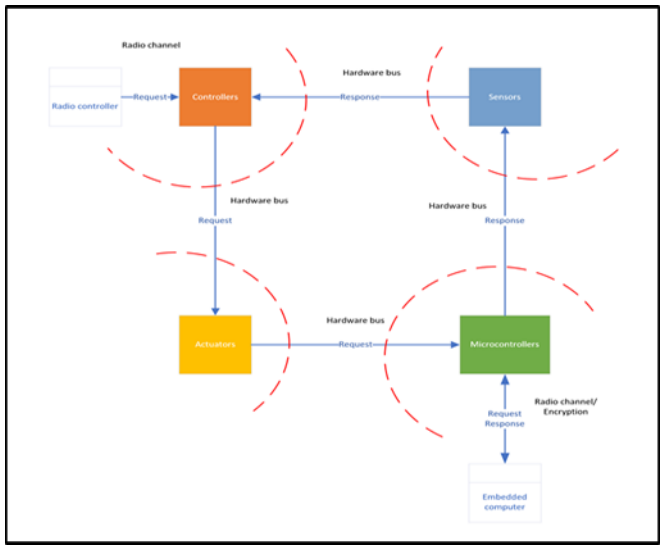


Data flow analysis applied in early stages of STPA



Data flow diagram when analyzing security early

VS.



Data flow diagram when analyzing security late

Several data flow elements, such as 4G, which are not directly linked to the control of the system are identified, which could easily be overlooked if we start security analysis late.

Conclusions

- STPA combined with other security threat modelling approach helped finding more security risks
- Starting thinking security in early stages of STPA helped find more security and safety risks
- Data flow diagram threat modelling approach fits better than others to be combined with STPA

Summary

RQ1: What is the security threat modeling analysis that can complement STPA-Sec best and easiest?

- Combing STPA with as misuse cases, attach trees, and Business Process Modelling Notation (BPMN) and data flow diagram can find different extra security threats.

RQ2: Start with security analysis, taking a base in the target assets related risks and consequences, and then consider safety afterward?

- Starting thinking security in early stages of STPA helped find more security and safety risks
- Data flow diagram threat modelling approach fits better than others to be combined with STPA

Key reference

- 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.