virtual vehicle

Enabling future vehicle technologies

Integration of safety and cybersecurity analysis through combination of systems and reliability theory methods

Joaquim M. Castella Triginer, Helmut Martin, Nadja Marko, Bernhard Winkler
Virtual Vehicle Research
Graz, Austria

10th EDITION EUROPEAN CONGRESS
ERTS 2020
FROM 29TH TO 31ST JANUARY / TOULOUSE FRANCE
PIERRE BAUDIS CONGRESS CENTER

Motivation

- Improve safety and cybersecurity analysis for:
  - Vehicles with strong E/E dependence
  - Critical systems (e.g. Drive-by-wire)
  - Limitations of the reliability analysis for complex systems
  - Automated/autonomous functionalities
  - Interconnectivity for automated/autonomous vehicles

Agenda

Motivation

Introduction

Integrated Safety and cybersecurity analysis

- **Methodology**
- **Case study:** Remote communication

Conclusion

Research center:

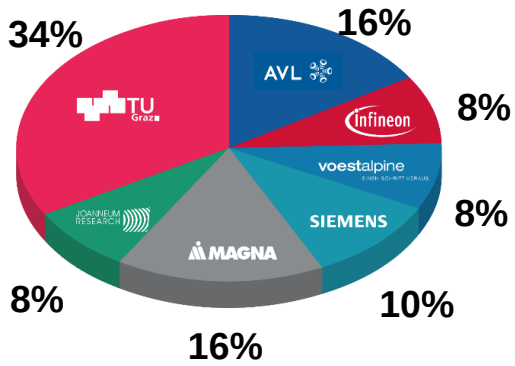
- Automated driving
- Advanced testing
- Digital operation
- Efficiency and comfort
- Efficient development
- Safety & security

FUNDED BY:

Das Land Steiermark · SFG · TU Graz Graz University of Technology

website: **www.v2c2.at**

SHAREHOLDERS:



GENERAL INFO:

Founded: **2002**

Staff: **~300**

Operating Income: **22 Mio. EUR**

Located in: **Graz, Austria**

Motivation

EU funding project: SECREDAS

- Development and Validation multi-domain architecting methodologies, reference architectures & components for autonomous systems
- Incorporation of high security and privacy protection while preserving functional-safety and operational performance

- https://secredas.eu/

Functional Safety Standards

- ISO 26262 (road vehicles)

Functional Cybersecurity Standards

- SAE J3061 (automotive cyber-physical systems)
- ISO/SAE 21434 (road vehicles)

STPA (Systems-Theoretic Process Analysis) Method

- Safety and Cybersecurity analysis technique based on systems theory
- Considers the overall role of the entire socio-technical system
- Hierarchical structures analyzed from the upper level to the lower level

ISO 26262

- Main interest on Concept Phase
- Partially on Product Development at the System Level

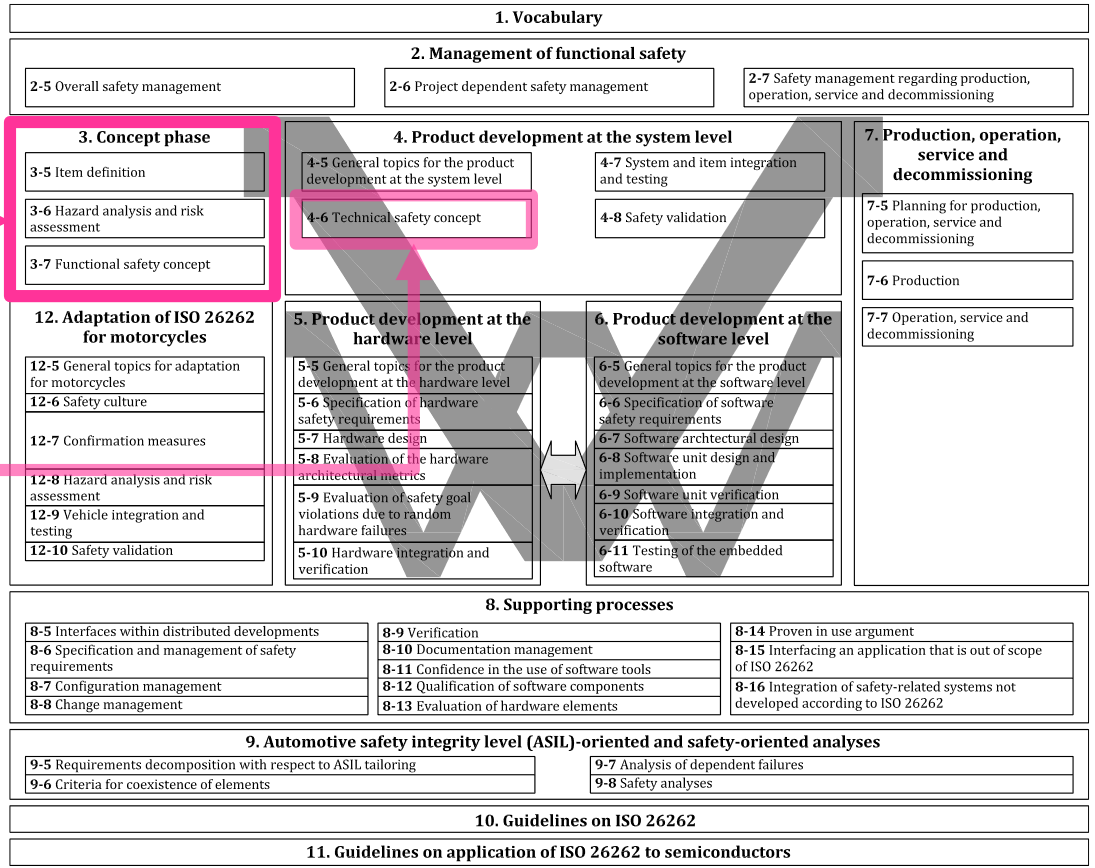


Figure 1 Overview of ISO 26262 [1]

SAE J3061

- Main interest on Concept Phase
- Partially on Product Development at the System Level

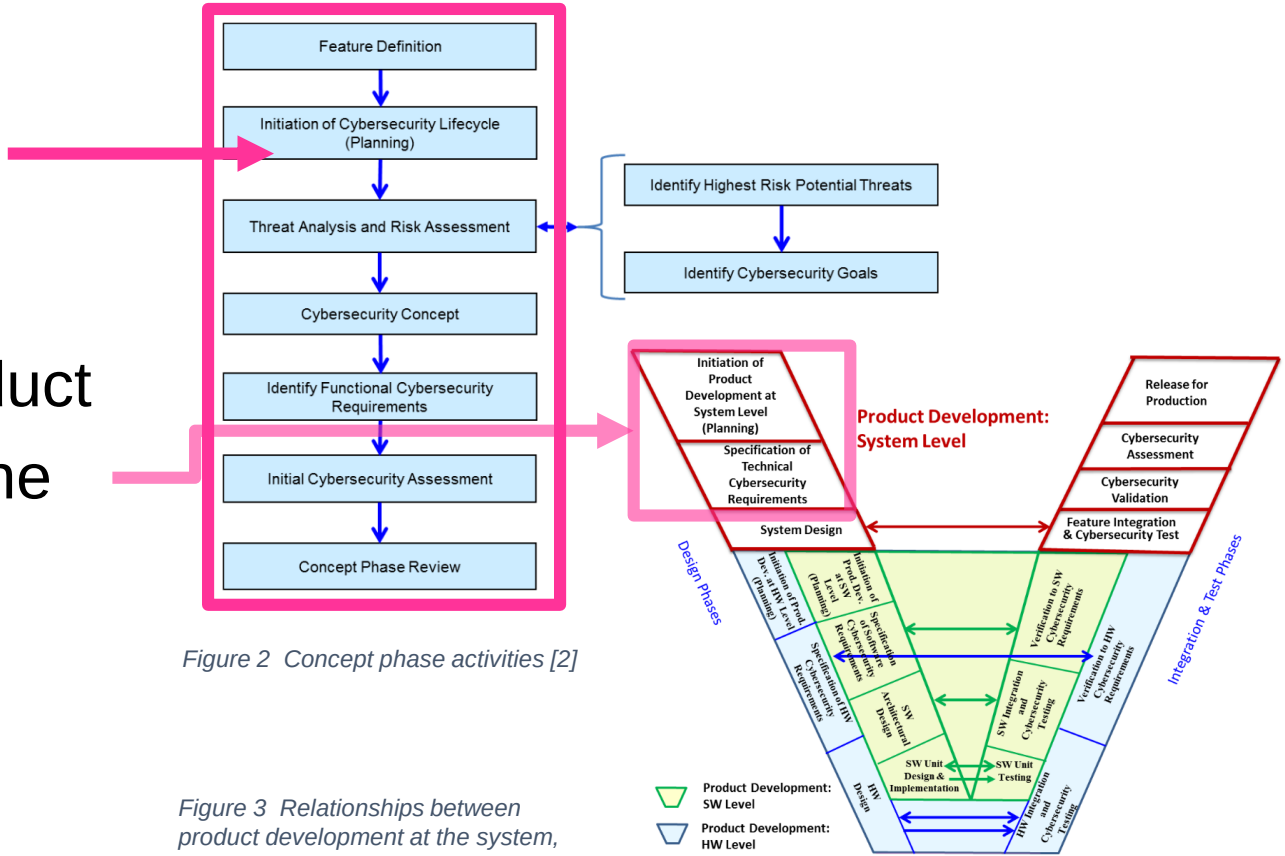


Figure 2 Concept phase activities [2]

Figure 3 Relationships between product development at the system, hardware, and software levels [2]

STPA

- Embodies the STAMP accident causality model (Systems Theoretic Accident Model & Processes)
- Losses are more than a chain of events, they involve complex dynamic processes
- Losses as a control problem, not a failure problem. Safety/Cybersecurity constraints are violated by inadequate control actions
- Losses often occur when the process model is incorrect, therefore controllers use a process model to determine control actions

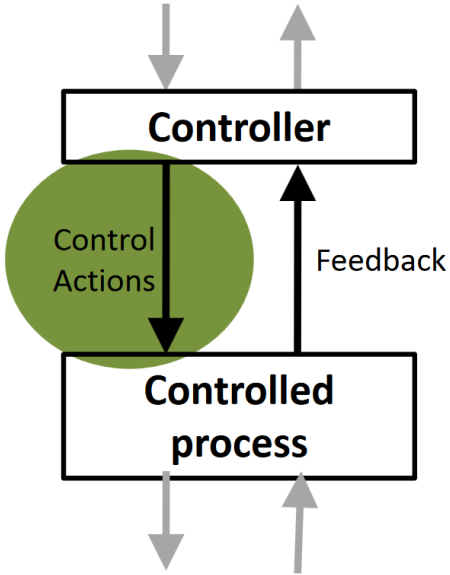


Figure 4 Generic control structure STPA [3]

STPA Workflow

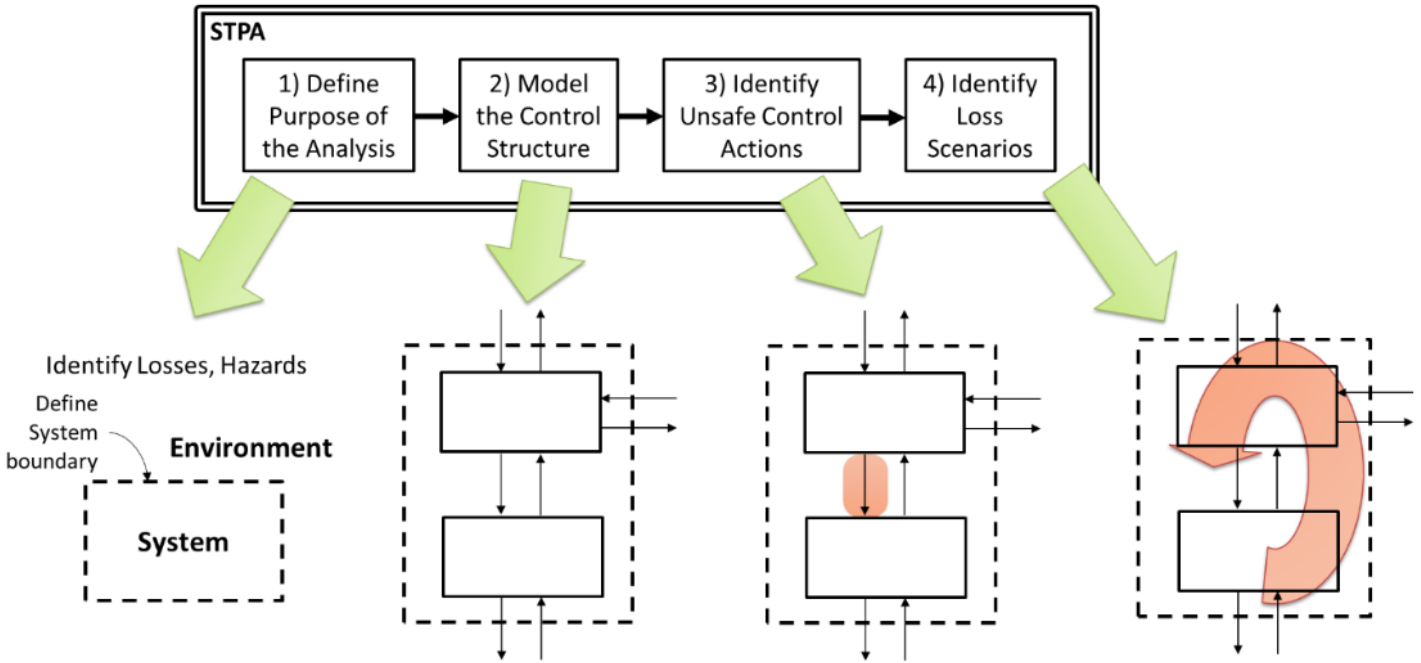


Figure 5 Overview of the basic STPA Method [4]

Integrated safety and cybersecurity analysis

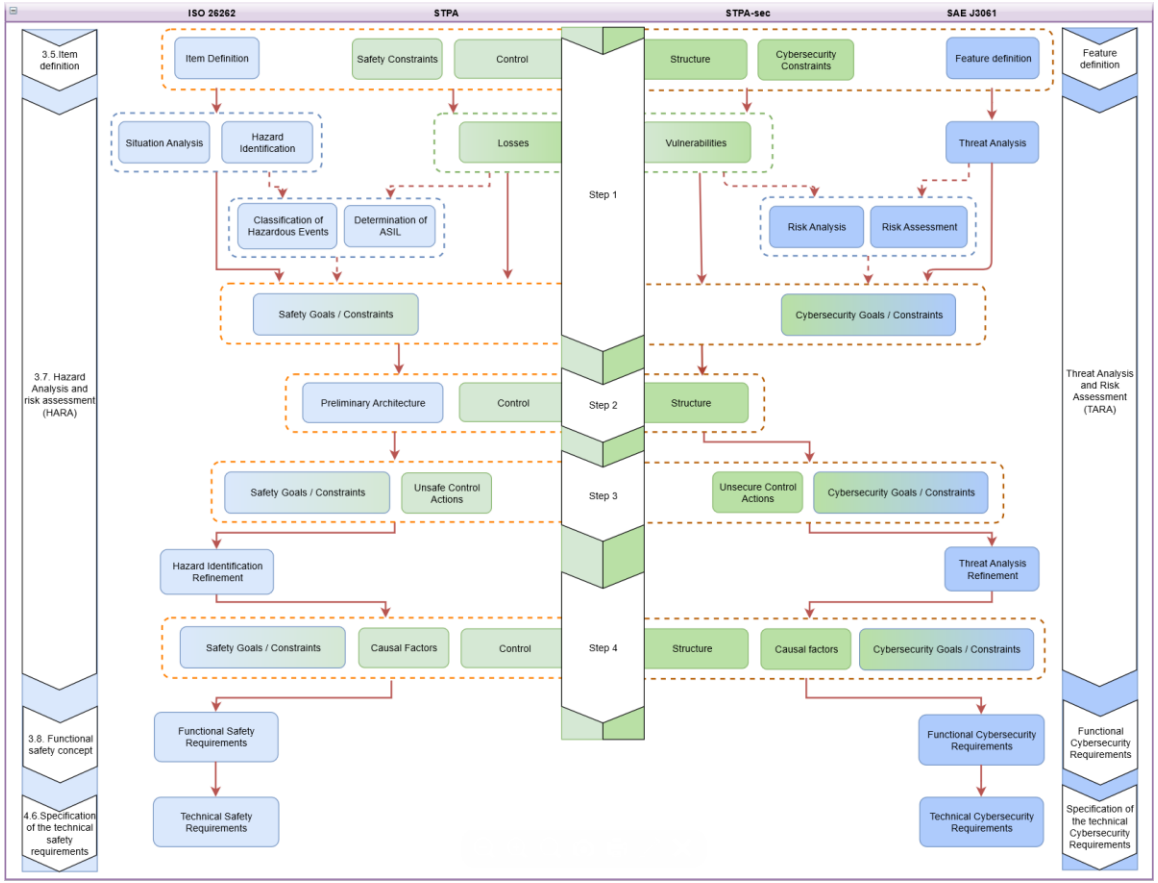
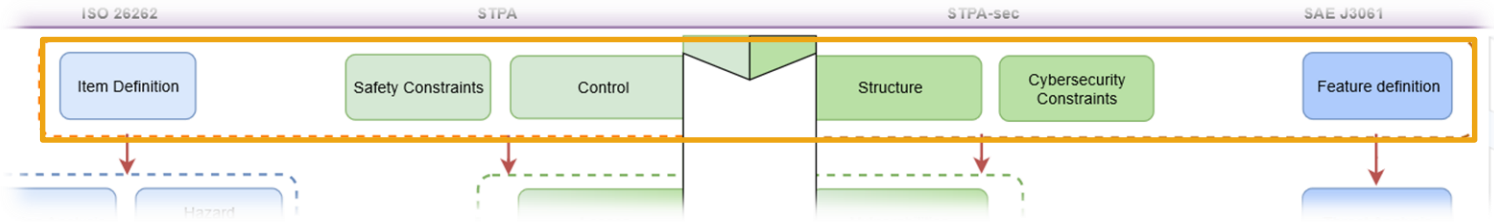
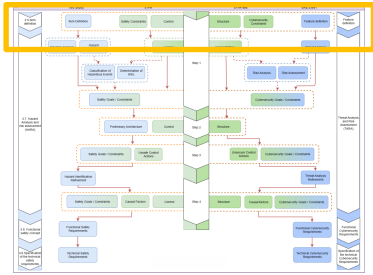


Figure 6 Integrated safety and cybersecurity analysis using STPA

Integrated safety and cybersecurity analysis





Item definition:

– ISO 26262: Description of item functionality, operation modes, states, operational and environmental constraints, legal requirements, assumptions and potential consequences of behavior shortfalls.

– SAE J3061: Called “Feature definition”, describe physical boundaries, cybersecurity perimeter and trust boundaries.

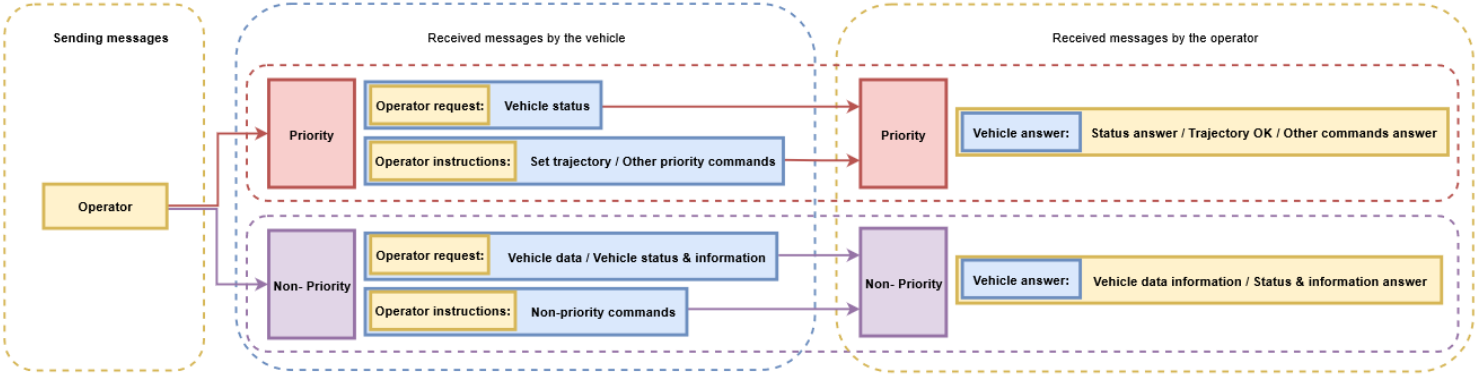
– STPA: Definition of the system boundaries and interactions between system and environment including human computer interactions.

Case study: Remote communication

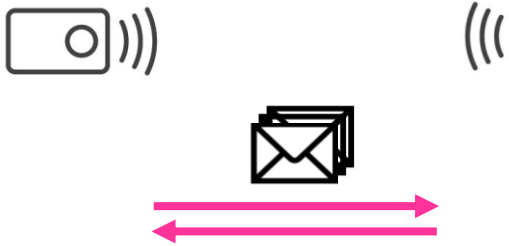
https://www.youtube.com/watch?v=ERIADfzx7T8

Case study: Remote communication

Remote communication architecture

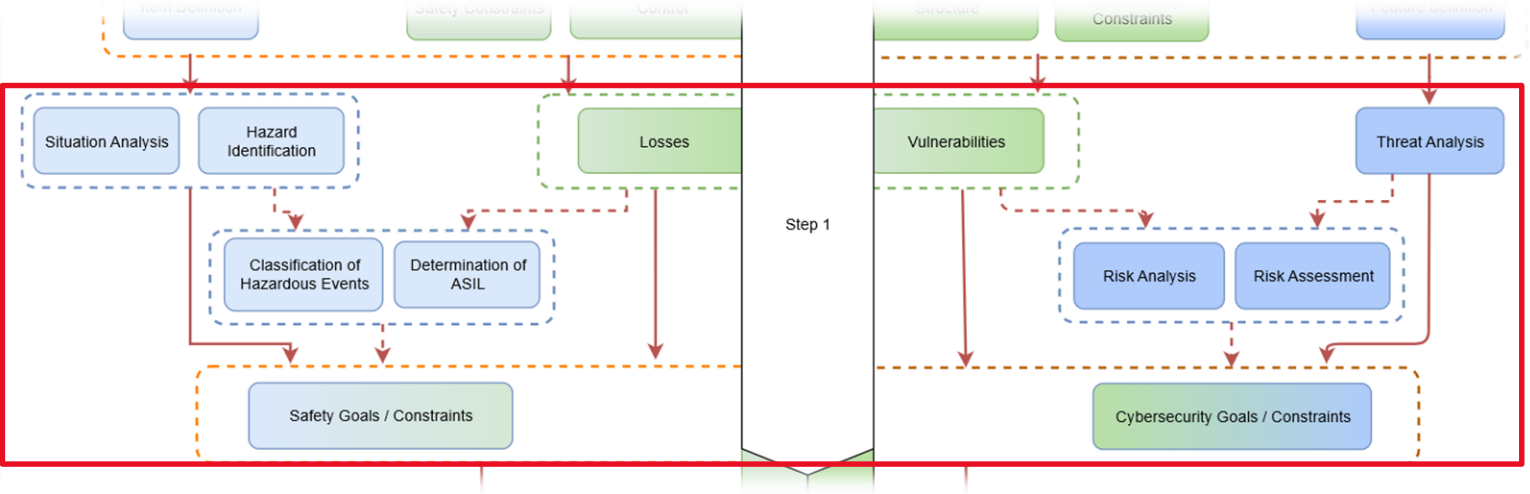


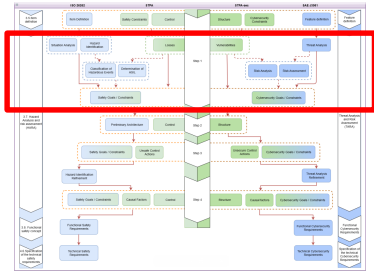
Remote operator



Vehicle

Integrated safety and cybersecurity analysis





Losses, Vulnerabilities, Threats and Hazards:

- ISO 26262: Operational situation and operating modes.
- STPA: Losses ordered by priorities or assigned level of severity.
- SAE J3061: Supports ISO 26262 adding cybersecurity analysis (EVITA, TVRA, OCTAVE, HEAVENS)

Case study: Remote communication

Losses, vulnerabilities and constraints

Losses

ID	Title
L-1	Human serious injury or loss of life
L-2	Loss of or damage to vehicle
L-3	Loss of or damage to objects outside/ins
L-4	Loss of customer satisfaction or compan
L-5	Loss of restricted information

ID	Title
L-1	Human serious injury or loss of life

Unified losses for safety and

Vulnerabilities

ID	Title	Links
V-1	Remote co	
V-2	Remote co	
V-4	Remote co	
V-5	A third agent takes information from the remote communication without authorization	L-4, L-5

ID	Title	Links
V-1	Remote communication is not sending or receiving signals	L-1, L-2, L-3, L-4

Extracted from losses, the generic

Specific cybersecurity vulnerabilities

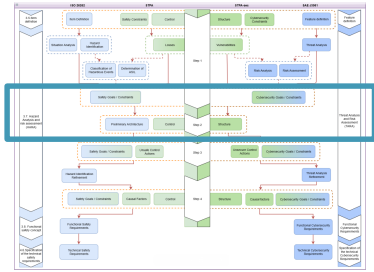
Safety and Security Constraints

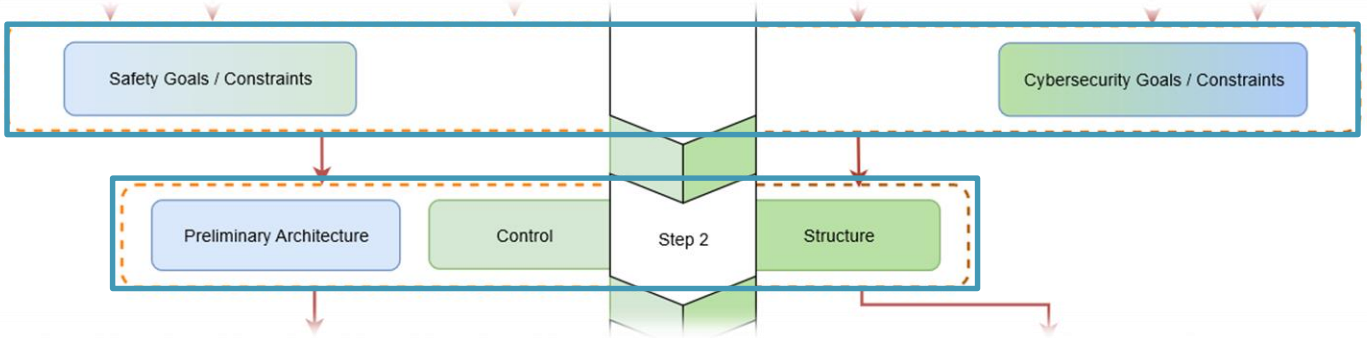
ID	Title
SC0.1	Remote communication must prev
SC0.2	Remote communication must prev
SC0.3	Remote communication must prev
SC0.4	Remote communication must verif
SC0.5	Remote communication must be between the vehicle and the operator without a third unauthorized agent

ID	Title
SC0.1	Remote communication must prevent the lack of availability of the signal

Integrated safety and cybersecurity analysis

The transformation of threats or hazard into safety or cybersecurity goals (ISO 26262 and SAE J3061) or constraints (STPA and STPA-sec)

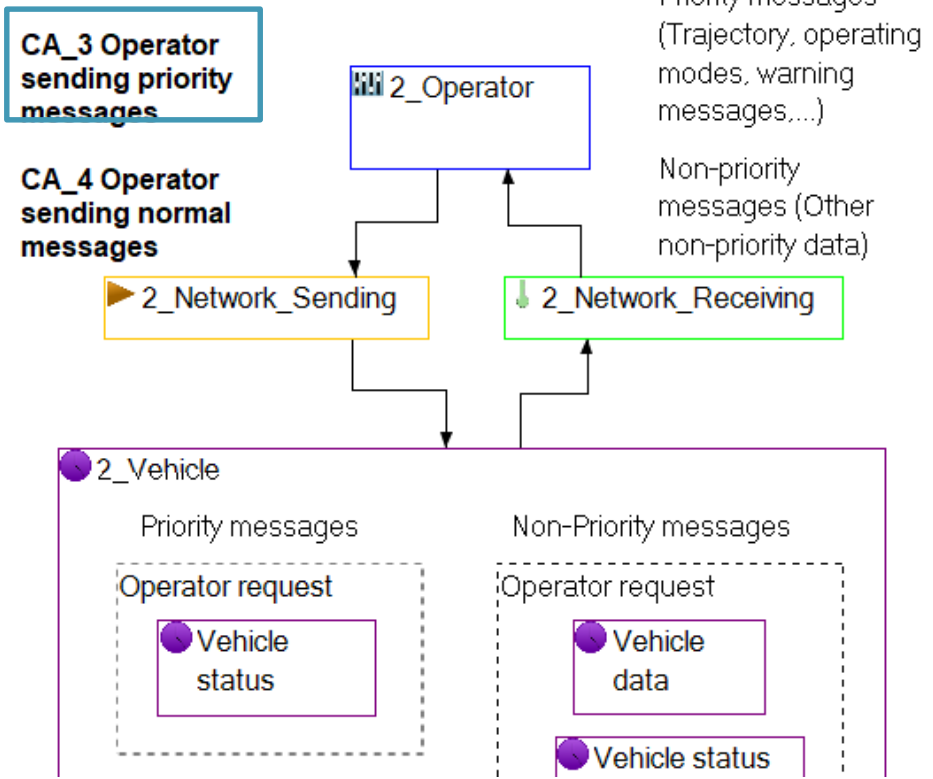


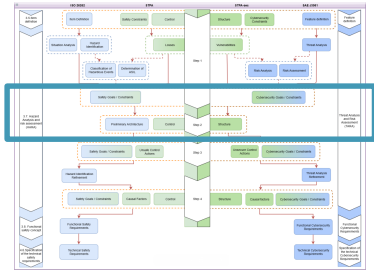


- Preliminary architecture should allocate functional safety requirements
- Control structure is a hierarchical system model representing the state of the controlled process

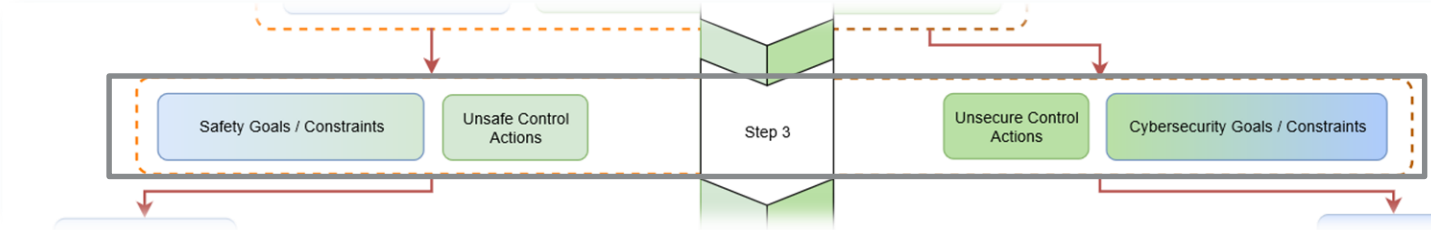
Case study: Remote communication

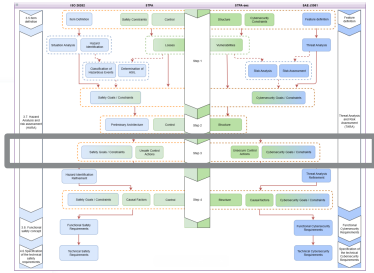
Control Structure





Integrated safety and cybersecurity analysis





- Identify unsafe/unsecure control actions:

Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long

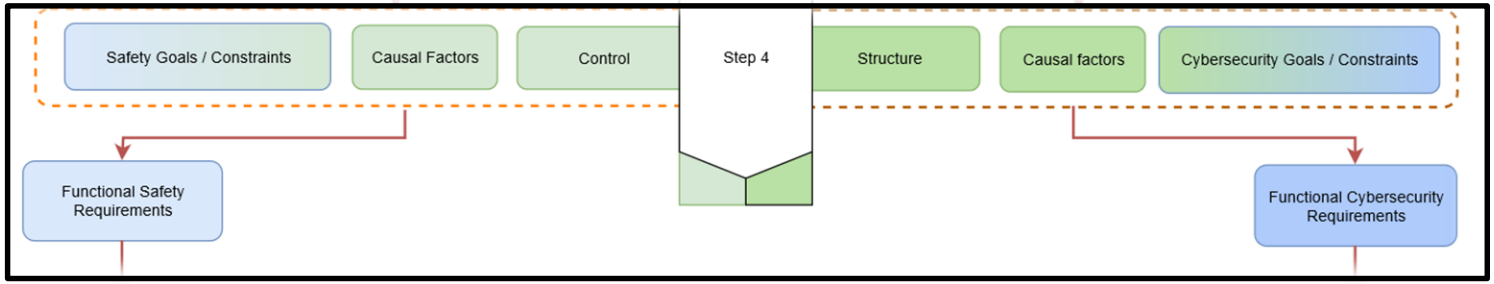
- Refinement of the safety and cybersecurity constrains/goals

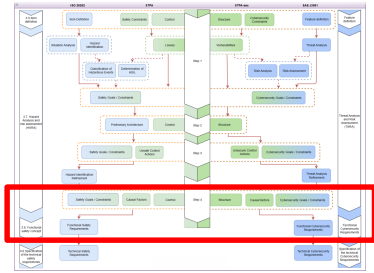
Case study: Remote communication

Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long
CA_3 Operator sending priority messages	UCA1.9	UCA1.10	UCA1.11	UCA1.12
	UCA_13 Operator is not sending priority messages when the vehicle status is required. (V-1) and (V-5)	UCA_16 Operator is sending incorrect priority messages when the vehicle status is required. (V-2), (V-3) and (V-4)	UCA_19 Operator is sending priority messages too late when the vehicle status is required. (V-1) and (V-2)	UCA_22 Operator is sending priority messages too long when the vehicle status is required. (V-1)
	[H-1]	[H-2] [H-3]	[H-1] [H-2]	[H-1]

- Priority message sent to vehicle
- Keywords to identify possible unsafe and unsecure control actions
- Traceability from the first hazard / vulnerability list
- Common unsafe and unsecure control action
- Different safety and cybersecurity constrains/goals

Integrated safety and cybersecurity analysis





- STPA: Identification of causal scenarios
  - Evaluation of the safety and cybersecurity constraints/goals
- ISO 26262 and SAE J3061:
  - Refinement of safety and cybersecurity functional requirements
  - Technical safety and cybersecurity requirements

Case study: Remote communication

Component	Unsafe Control Action	Causal Factor	Hazard Links	Causal Scenarios	Safety Constraint	Notes / Rationale
2_Operator	UCA1.13					
	Operator is not sending priority messages when an instruction is required	Operator thinks that priority messages are sent correctly	H-1	The operator sends a new trajectory as instruction through a priority message that, during message generation, get lost without being sent.	The operator must guarantee the priority communication signal with the vehicle when a trajectory instruction is sent. The operator must contain some error management methods to detect faults in sending priority messages. Otherwise, if the operator does not send a message in less than 20 ms, the operator must warn the system that the vehicle is in danger.	Note/Rational...

- Scenarios are derived till have the complete safety and cybersecurity goals
- The list is extended with 24 safety goals and 50 cybersecurity goals for UCA

Conclusion

- Integrate safety and cybersecurity analysis using STPA
  - One common analysis model
  - Impact of security on safety

- STPA is an additional analysis method that extends safety and security analysis proposed in the standards
  - Better system understanding
  - Additional safety and security requirements
  - Verification of previous safety and security analyses results

Outlook

- Evaluation of applicability of STPA approach:
  - Which kind of systems
    - Safety/security critical systems
    - High interconnected systems (E/E architectures) (in vehicle communication)
    - Systems with external connectivity where security has a big impact on the safety
  - When do you want to apply?
    - Safety critical (ASIL A to D?)
    - Security impact on safety
  - Is it applicable for product development on the system level?

virtual vehicle

Enabling future vehicle technologies

THE END

Joaquim Maria Castella Triginer
Joaquim.castellatriginer@v2c2.at
Researcher / Dependable systems

ERTS2020

www.v2c2.at

Virtual Vehicle Research GmbH is funded within the COMET – Competence Centers for Excellent Technologies – programme by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT), the Federal Ministry for Digital and Economic Affairs (BMDW), the Austrian Research Promotion Agency (FFG), the province of Styria and the Styrian Business Promotion Agency (SFG). The COMET programme is administrated by FFG.

Bibliography

[1] [ISO 26262, “Road vehicles – Functional safety,” second edition, 2018]

[2] [SAE J3061, “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems Road Vehicles,” 2016]

[3] [J. Thomas, “Introduction to system safety and risk management in complex systems,” Massachusetts Institute of Technology, 2014.]

[4] [N. G. LEVESON and J. P. THOMAS, STPA handbook, 2018]

Agenda

Motivation: ensuring safety and security of future cars

Introduction: safety and cybersecurity on automotive industry

Methodology: safety and cybersecurity analysis

Use Case: remote communication of SPIDER

Results: integrate safety and cybersecurity analysis using STPA

Conclusion: method that extends safety and cybersecurity

Presented approach

Losses

ID	Title
L-1	Human serious injury or loss of life
L-2	Loss of or damage to vehicle
L-3	Loss of or damage to objects outside/inside the vehicle
L-4	Loss of customer satisfaction or company reputation
L-5	Loss of restricted information

Vulnerabilities

ID	Title	Links
V-1	Remote communication is not sending or receiving signals	L-1, L-2, L-3, L-4
V-2	Remote communication is sending or receiving signals incompletely	L-1, L-2, L-3, L-4
V-3	Remote communication is sending or receiving corrupted signals	L-1, L-2, L-3, L-4
V-4	Remote communication is sending or receiving signals from unauthorized operators	L-1, L-2, L-3, L-4, L-5
V-5	A third agent takes information from the remote communication without authorization	L-4, L-5

Safety and Security Constraints

ID	Title
SC0.1	Remote communication must prevent the lack of availability of the signal
SC0.2	Remote communication must prevent the lack of the completeness of the signal.
SC0.3	Remote communication must prevent the lack of the integrity of the signal
SC0.4	Remote communication must verify that the signal is authorized.
SC0.5	Remote communication must be between the vehicle and the operator without a third unauthorized agent

Unified losses for safety and cybersecurity, ranked and prioritized by severity

Extracted from losses, the generic vulnerabilities applicable to both safety and cybersecurity

Specific cybersecurity vulnerabilities

Integrated list of safety and cybersecurity constraints

ISO 26262

- ISO 26262 is an international standard for functional safety of electrical and/or electronic systems in production automobiles
- Released in 2011, updated in 2018
- Addresses:
  - Safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles
  - Possible hazards caused by malfunctioning behavior of safety-related E/E systems, including interaction of these systems
  - Describes a framework for functional safety to assist the development of safety-related E/E systems and integrate functional safety activities into a company-specific development framework.

SAE J3061

- SAE J3061 establishes a set of high-level guiding principles for cybersecurity as it relates to automotive cyber-physical systems to be utilized in series production
- Includes:
  - Defining a framework for a lifecycle process to incorporate cybersecurity into automotive cyber-physical systems.
  - Providing information on some common tools and methods used when designing and validating cyber-physical automotive systems.
  - Providing basic Guiding Principles on Cybersecurity for Automotive Systems.
  - Providing the foundation for further standards development activities in vehicle cybersecurity.

Conclusion

- Integrate safety and cybersecurity
- Combine systems and reliability theory methods
- Use case is presented to carry out the analysis and provide results to validate the analysis.
- Refinement of the SPIDER remote communication requirements
- Unification of safety and cybersecurity constraints helps to interconnect both properties and to address integrated analysis on cyber-physical systems

Extension

- Properties or attributes that connect safety and cybersecurity
- Identification of causal factors in the last step of STPA analysis
  - The causal factor step presents a lack of cybersecurity support that forces the paper to introduce other cybersecurity models such as STRIDE.

Extension

Integrate safety and cybersecurity
Combine systems and reliability theory methods
Use case is presented to carry out the analysis and provide results to validate the analysis.
Refinement of the SPIDER remote communication requirements
Unification of safety and cybersecurity constraints helps to interconnect both properties and to address integrated analysis on cyber-physical systems

The first problem is related to the properties or attributes that connect safety and cybersecurity. The results cannot provide a clear representation of the relations between both properties or attributes. The second problem arises in the identification of causal factors in the last step of STPA analysis. The causal factor step presents a lack of cybersecurity support that forces the paper to introduce other cybersecurity models such as STRIDE. Nevertheless, these last two points will be covered in future extensions.