INTEGRATING SAFETY AND SECURITY FOR CYBER-PHYSICAL SYSTEMS

GIEDRE SABALIAUSKAITE
Associate Professor, Systems Security Group,
Institute of Future Transport and Cities (IFTC), Coventry University, UK

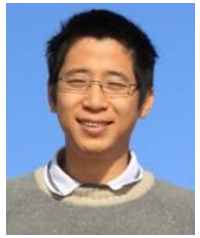
Seminar@SystemX
11th February 2021

Research Institute
Future Transport and Cities
Coventry University

Our team – Systems Security Group (SSG)

Siraj Shaikh
(Professor)

Giedre Sabaliauskaite
(Associate Professor)

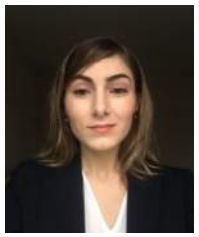


Hoang Nga Nguyen
(Assistant Professor)

Jeremy Bryans
(Assistant Professor)

Farhan Ahmad
(Assistant Professor)

Alistair Robertshaw
(RF Research Engineer)



Kristen Kuhn
(Research Assistant)

Hesamaldin Jadidbonab
(Research Fellow)

Andrew Tomlinson
(Research Fellow)

Research Students

- Sean Taylor
- Rhys Kirk
- Shahid Mahmood
- Mike Waters
- Kacper Sowka
- Oluwole Sowunmi
- Luis-Pedro Cobos
- Stephen Powley
- Matthew Holland
- Jeptoo Kipkech
- Ahmed Khan
- Shahzad Alam

Our Mission

Our core mission is to **research** and **engineer** secure and resilient cyber-physical systems for automotive and transport industry, working in collaboration with partners in industry, academia and government

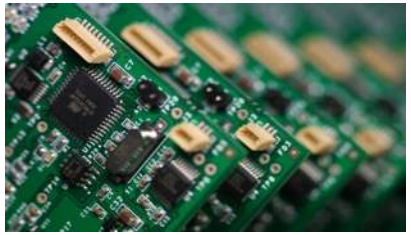
Sample Projects

SECURE CAV

Funding: £2.8M
Duration: November 2019 – November 2021

Partners: Mentor (part of Siemens), University of Southampton, Copper Horse Ltd.

SecureCAV is developing the world's first on-chip and in-life monitoring solution to detect system anomalies at clock-speed, be vendor-neutral, non-intrusive, runtime configurable and far less prone to hacking



As part of this, SSG is building a dedicated hardware-in-the-loop testbed for automotive cybersecurity threat detection and in-life vehicle monitoring techniques

5G CAL

5G Enabled Connected Autonomous Vehicle Logistics

Funding: £4.9M
Duration: August 2020 – March 2022

Partners: North East Automotive Alliance, Sunderland City Council, Newcastle University, Vantec, Connected Places Catapult, StreetDrone, and Perform Green

The project is testing self-driving heavy goods vehicles to evaluate how 5G connectivity can improve productivity through enhanced transport and logistics

SSG will undertake a thorough cybersecurity assessment of 5G connectivity and remote operation of vehicle control

Safety and security integration

Photo by Matthew Lancaster on Unsplash

Safety and security

- Safety and security are two crucial properties (qualities) of systems
  - **Safety**: protecting the systems from **accidental** failures
  - **Security**: protecting the systems from **intentional** attacks (physical and cyberattacks)
- They both are dealing with the minimization of risk of an undesired outcome
- They are inter-dependent, often complementing or conflicting each other

Photo by Kris Mikael Krister on Unsplash

Examples of Conflicts between Safety and Security

Photo by Michael Skok on Unsplash

Photo by Duy Hoang on Unsplash

Three Key Questions

1. How can we **IDENTIFY** inter-relationships between safety and cybersecurity?

2. How can we **CAPTURE** the inter-relationships between safety and cybersecurity?

3. How can we **SOLVE CONFLICTS** between safety and cybersecurity?

iTrust Centre for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Research Institute Future Transport and Cities | Coventry University

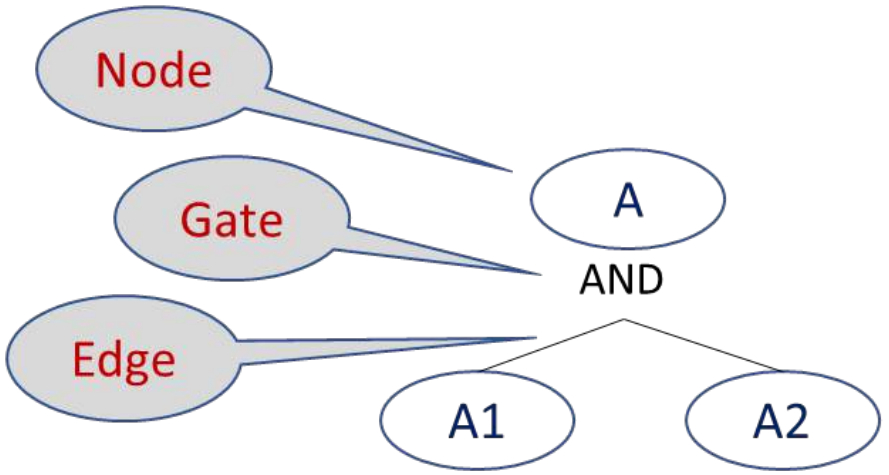
Question 1

How can we IDENTIFY inter-relationships between safety and cybersecurity?

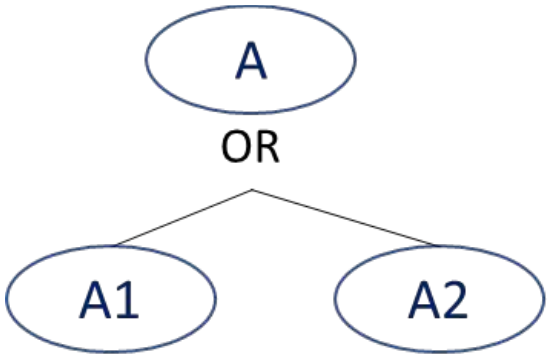
Photo by Brian Jones on Unsplash

Fault Trees for Safety Modelling

- **Fault tree** analysis is a widely used technique for hazard and risk assessment
- Purpose – to graphically present the possible events that can cause top-level undesired event



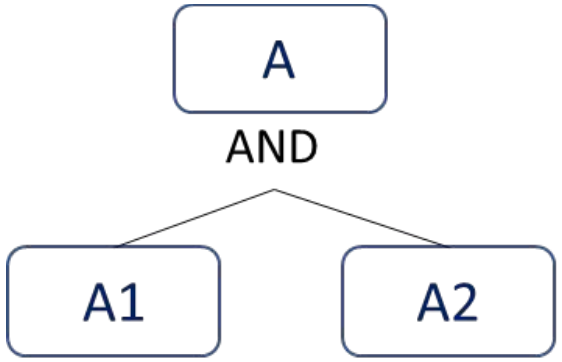
*A occurs if **both** A1 and A2 occur*



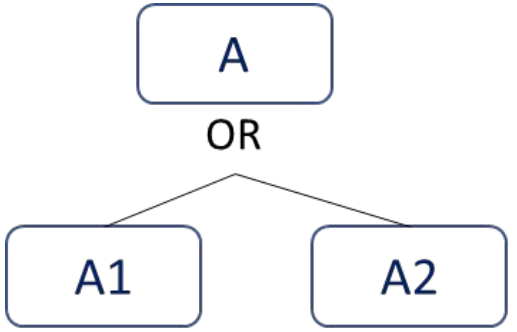
*A occurs if **either** A1 **or** A2 occurs*

Attack Trees for security modelling

- **Attack trees** are frequently used for security analysis
- Attack tree is a graph that describes the steps of attack process
- It uses the same basic symbols as fault tree

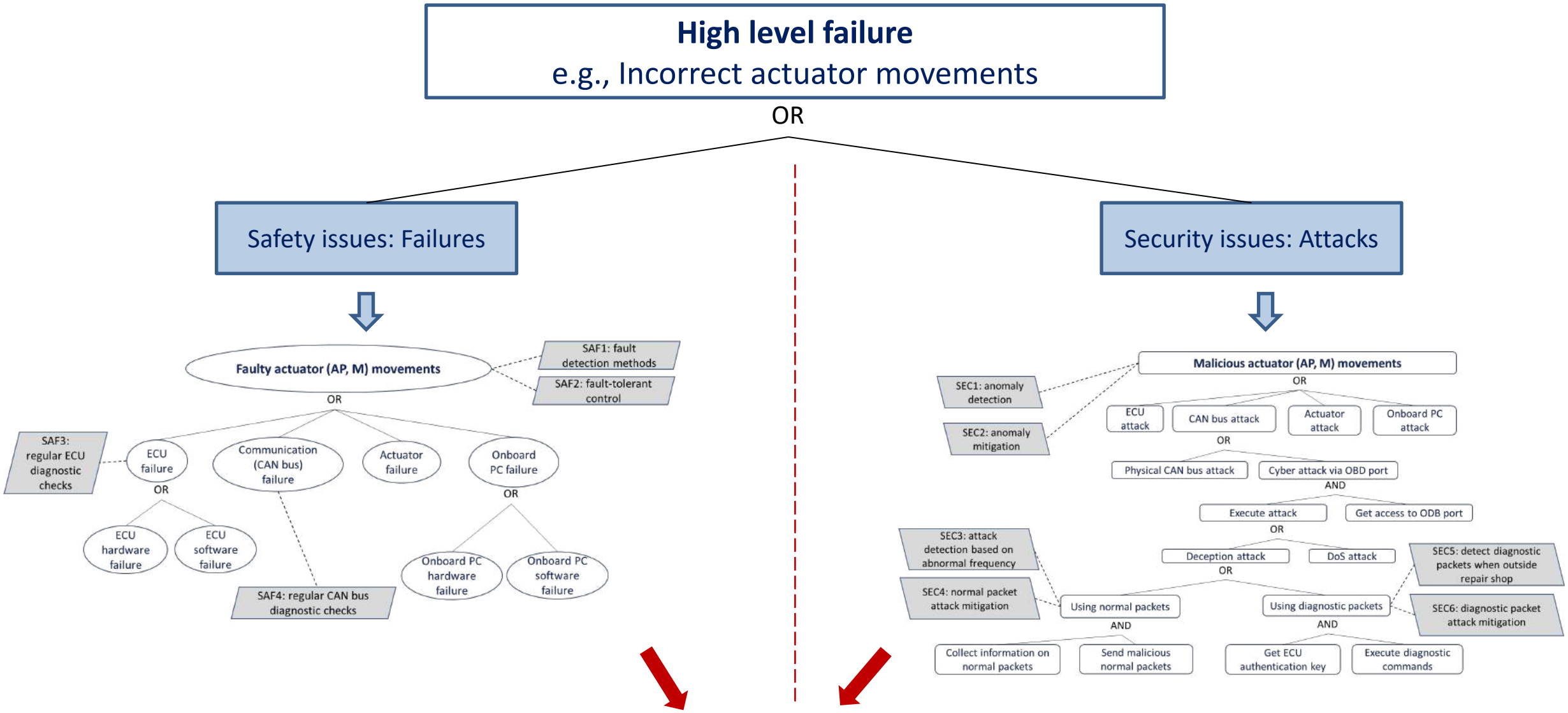


*To succeed with attack A, **both** A1 and A2 have to be successful*



*To succeed with attack A, **either** A1 **or** A2 have to be successful*

Conventional approach: safety and security are analyzed independently

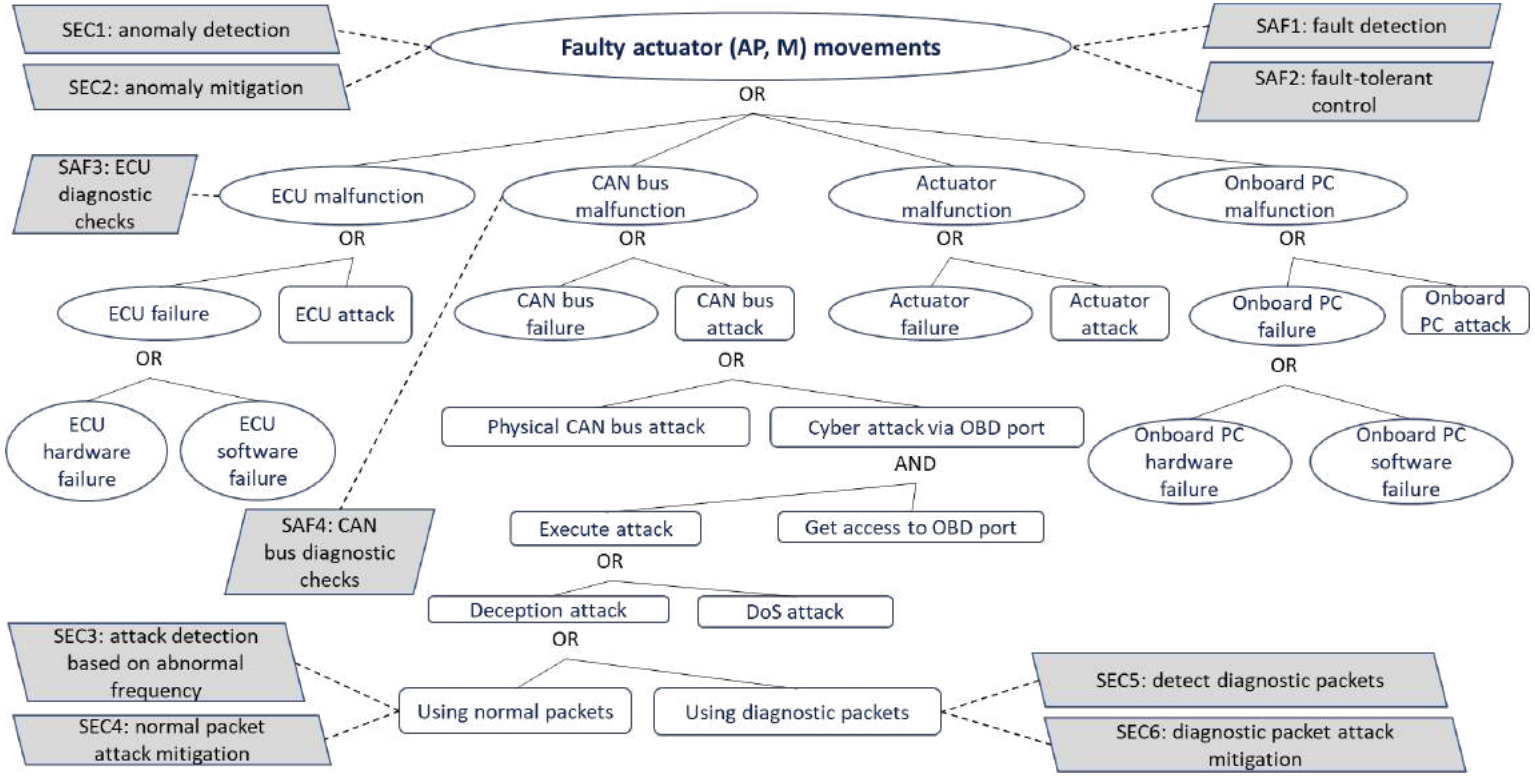


Combine into one model?

Model 1: FACT (Failure Attack CounTermeasure) Graph

The **FACT graph*** can be used to

- "see" a complete picture of "weaknesses" of the system
- analyze the coverage of attacks and failures by safety and security countermeasures
- Identify missing and overlapping countermeasures



**Sabaliauskaite G., Mathur A.P. (2015) Aligning Cyber-Physical System Safety and Security. In: Cardin MA., Krob D., Lui P., Tan Y., Wood K. (eds) Complex Systems Design & Management Asia. Springer, Cham.*

Question 2

How can we CAPTURE the inter-relationships between safety and cybersecurity?

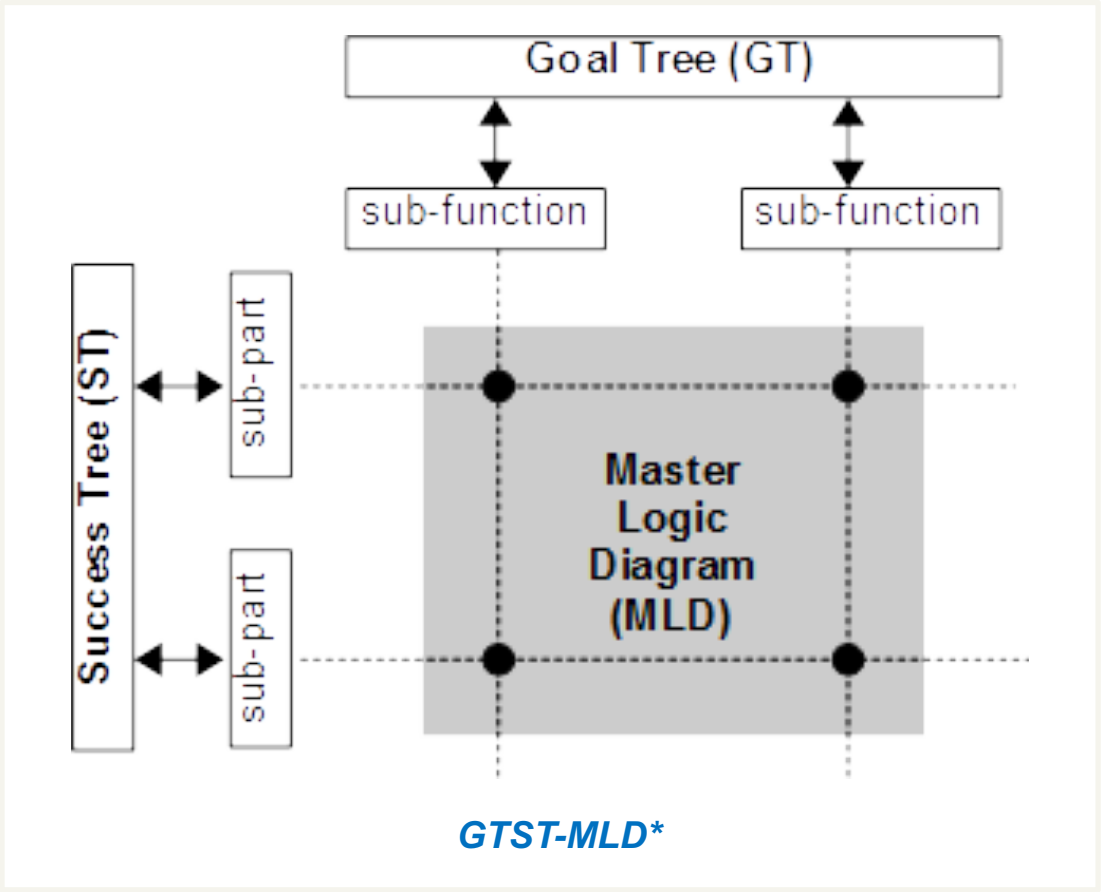
Photo by Brian Jones on Unsplash

Hierarchical approaches: GTST-MLD*

In 1980s, **GTST** (Goal Tree Success Tree) framework has been introduced for modelling complex physical systems

- The main idea behind GTST is that complex systems can be best describe by hierarchies
- Goal Tree (GT) – hierarchy of system functions
- Success Tree (ST) – hierarchy of system components

In 1999, Modarres and Cheon extended GTST and added Master Logic Diagram (**MLD**) to capture inter-relationships between GT and ST



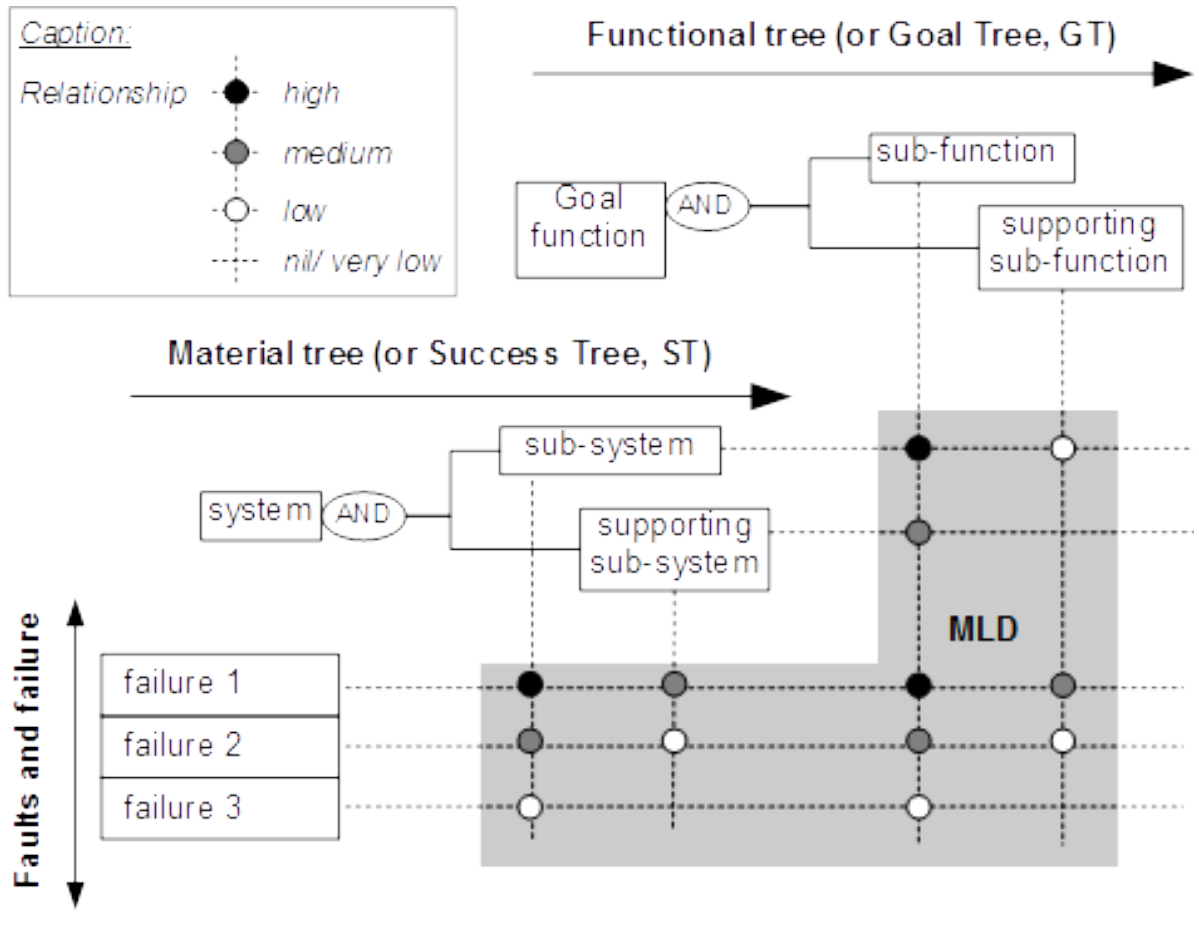
GTST-MLD*

**Modarres, M., Cheon, S.W.: Function-centered modeling of engineering systems using the goal tree - success tree technique and functional primitives. Reliability Engineering & System Safety 64(2), 181-200 (1999)*

Extension of GTST-MLD: 3-Step Model

In 2009, Brissaud et al. extended GTST-MLD for safety analysis by integrating failures into it, and developed the **3-Step Model**

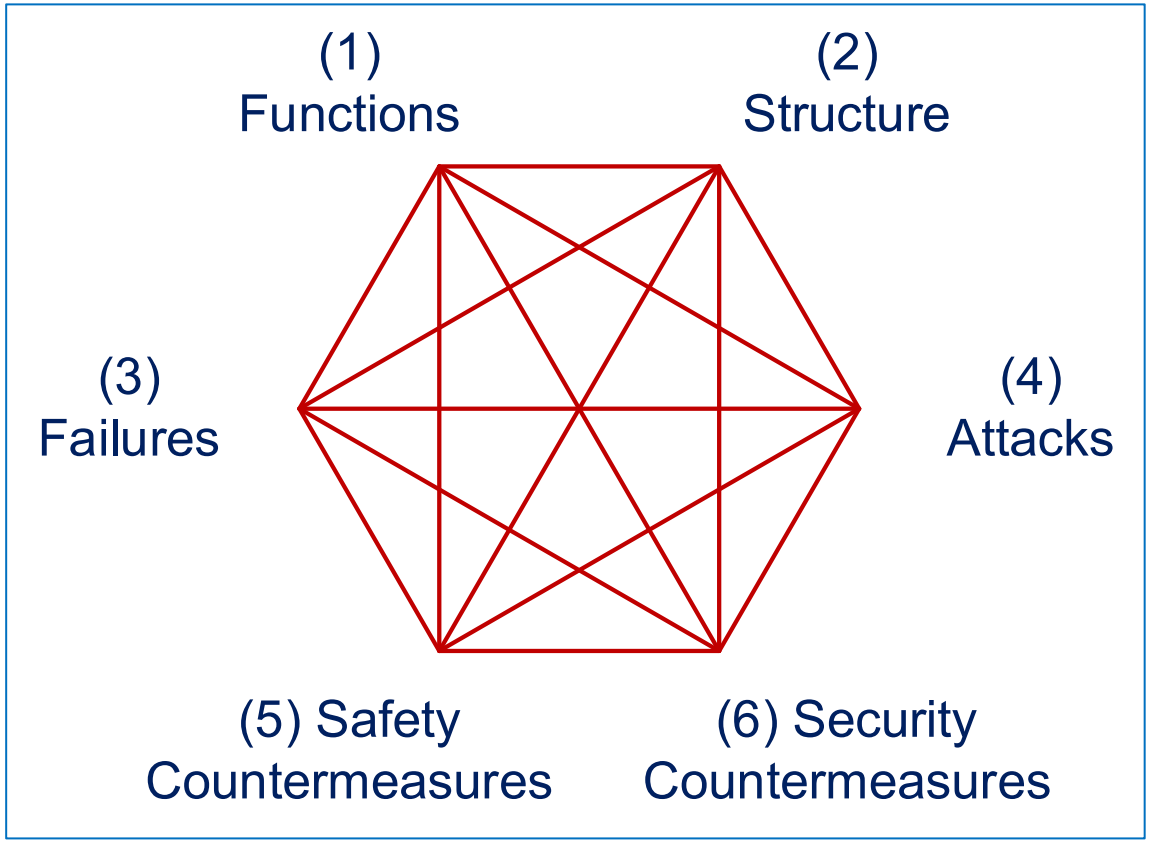
Can we use similar approach for capturing the relationships between safety and security?



*The 3-Step**

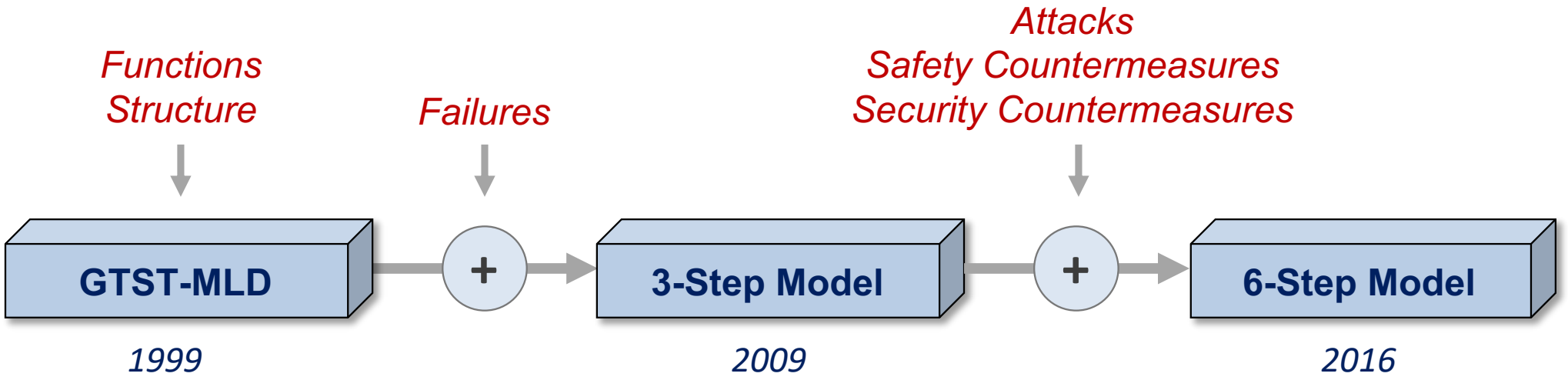
Brissaud, F., Barros, A., Bererenguer, C., Charpentier, D.: Reliability study of an intelligent transmitter. In: 15th ISSAT International Conference on Reliability and Quality in Design. pp. 224-233. International Society of Science and Applied Technologies (2009)

What information could we use to describe the relationships between safety and security?



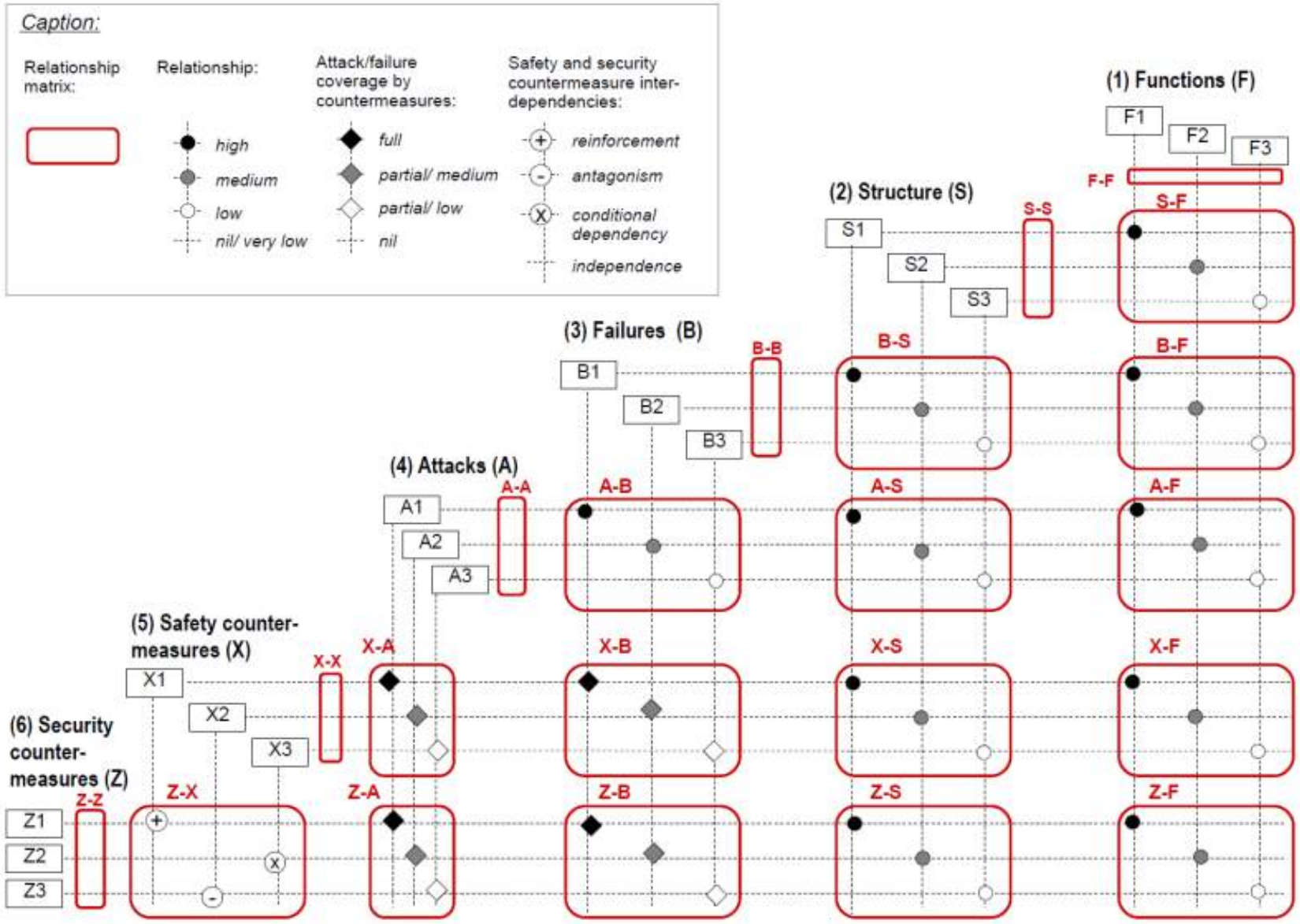
Further extension of the 3-Step Model for integrated analysis of relationship between safety and security

- In 2016, we extended the 3-Step Model and added the attacks, safety countermeasures, and security countermeasures
- As a result, the **Six-Step Model** was developed



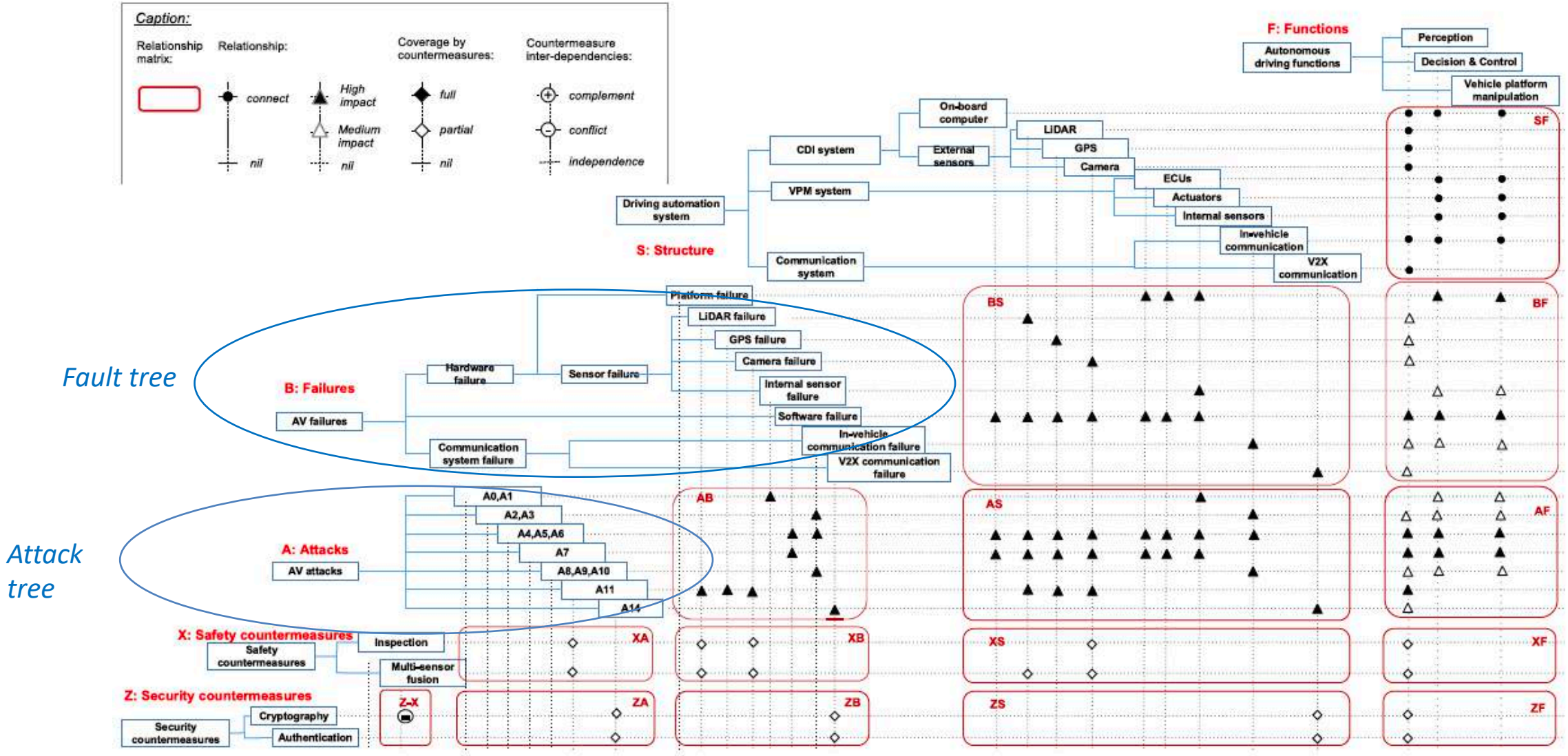
Model 2:
Six-Step Model*

Consists of:
- ✓ *6 hierarchies*
- ✓ *21 relationship matrices*



**G. Sabaliauskaite, S. Adepu, and A. Mathur, "A six-step model for safety and security analysis of cyber-physical systems," in the 11th International Conference on Critical Information Infrastructures Security (CRITIS), Oct 2016.*

Six-Step Model Example*



J. Cui, G. Sabaliauskaite, L. S. Liew, F. Zhou and B. Zhang, "Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles," in IEEE Access, vol. 7, pp. 148672-148683, 2019

Question 3

How can we SOLVE CONFLICTS between safety and cybersecurity?

Photo by Brian Jones on Unsplash

Which quality is more important: safety or security?

Photo by Jean Wimmerlin on Unsplash

Which quality is more important: safety or security?

None…

they both are equally important to meet organization's business goals

Photo by Jean Wimmerlin on Unsplash

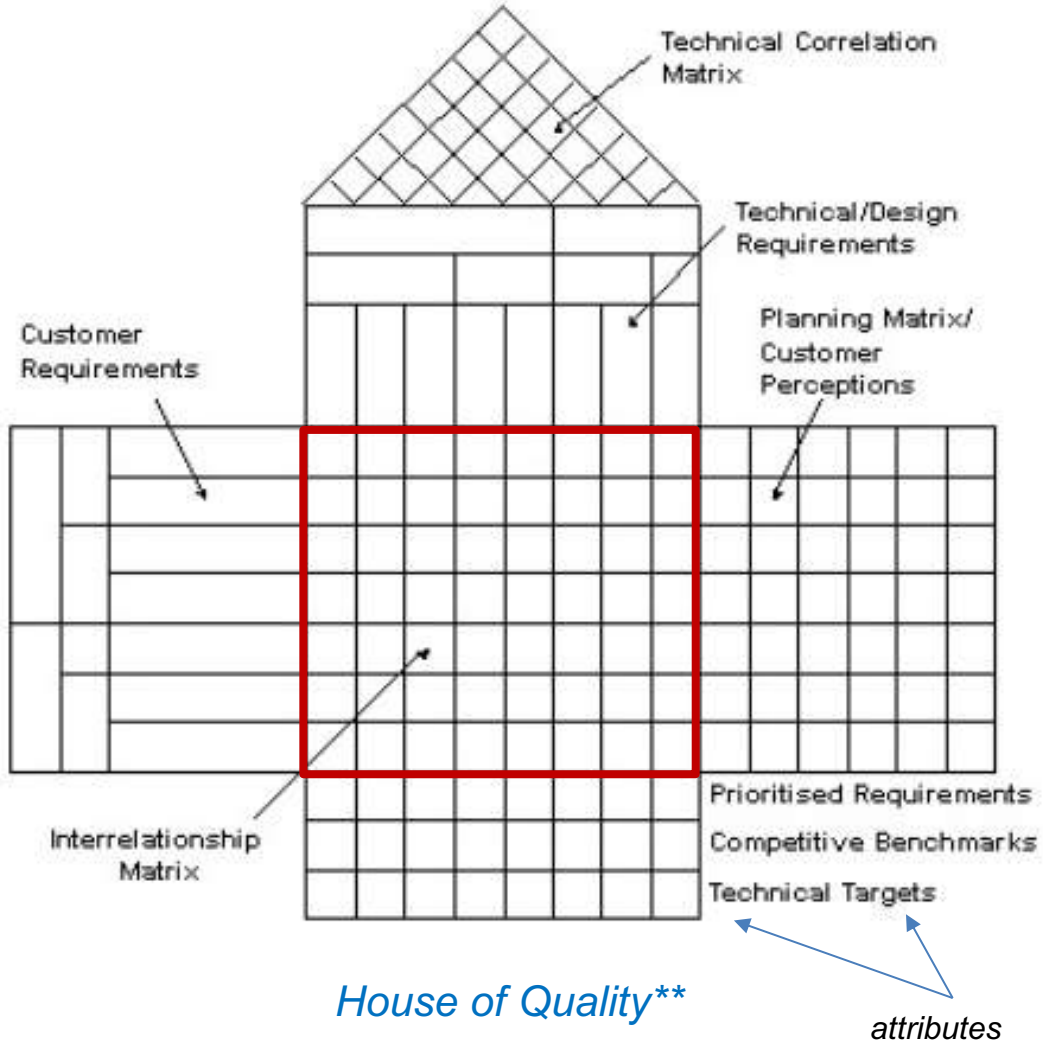
Decision making method: Quality Function Deployment (QFD)

QFD* was created in Japan in the late 1960s

- a method for structured product planning and development
- effective in reducing development time and cost
- useful for recording the considerations/decisions

QFD utilizes a series of matrices to transform qualitative customer requirements into detailed engineering specifications

- QFD matrix, namely House of Quality (HoQ), displays the relationships between dependent (WHATs) and independent (HOWs) variables
- WHATs are included as rows of HoQ, while HOWs – as columns
- Various attributes of WHATs and HOWs can be used to support decision making

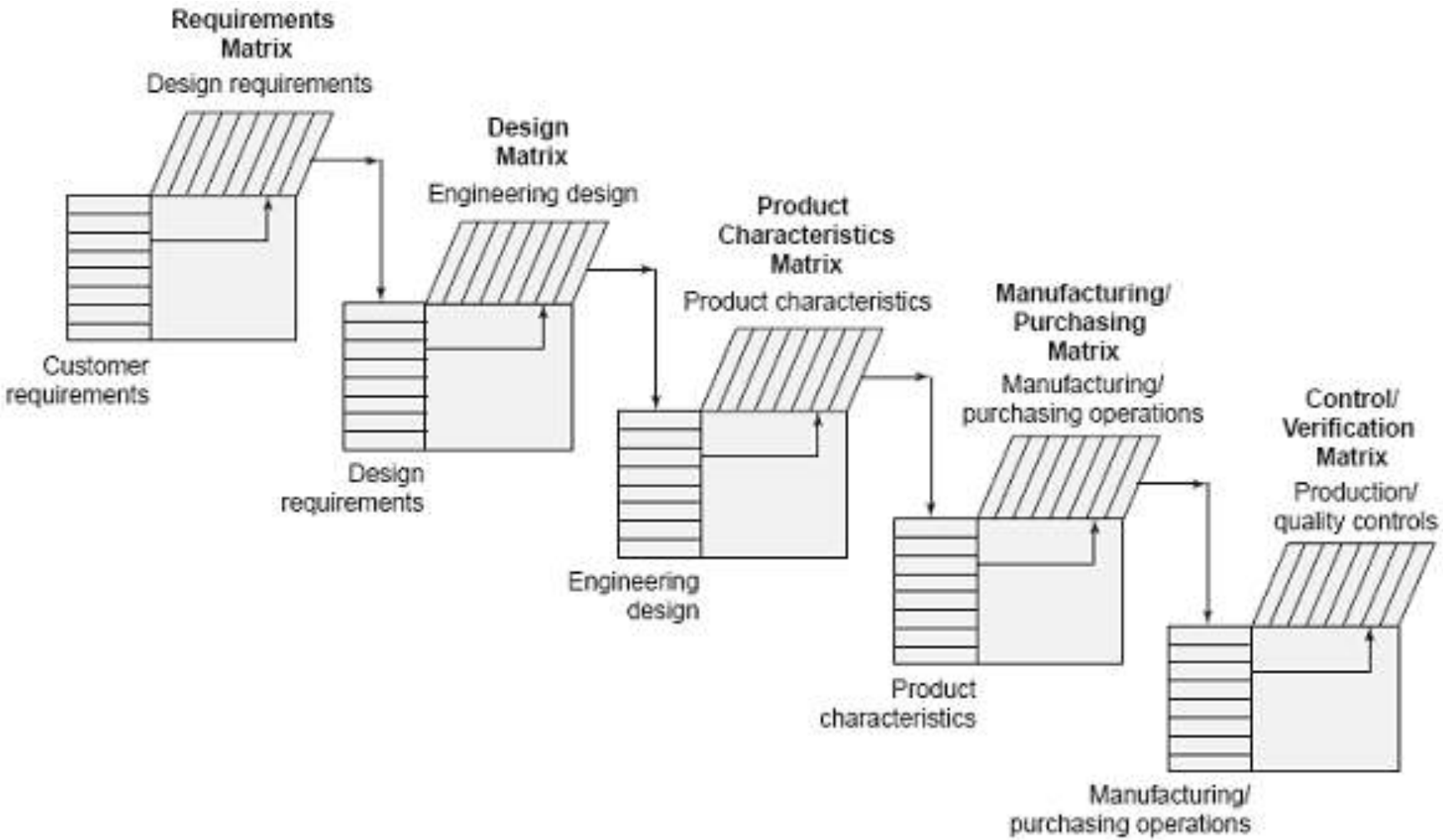


*House of Quality***

** T. Cohen. Quality function deployment. American Management Association. 1994*

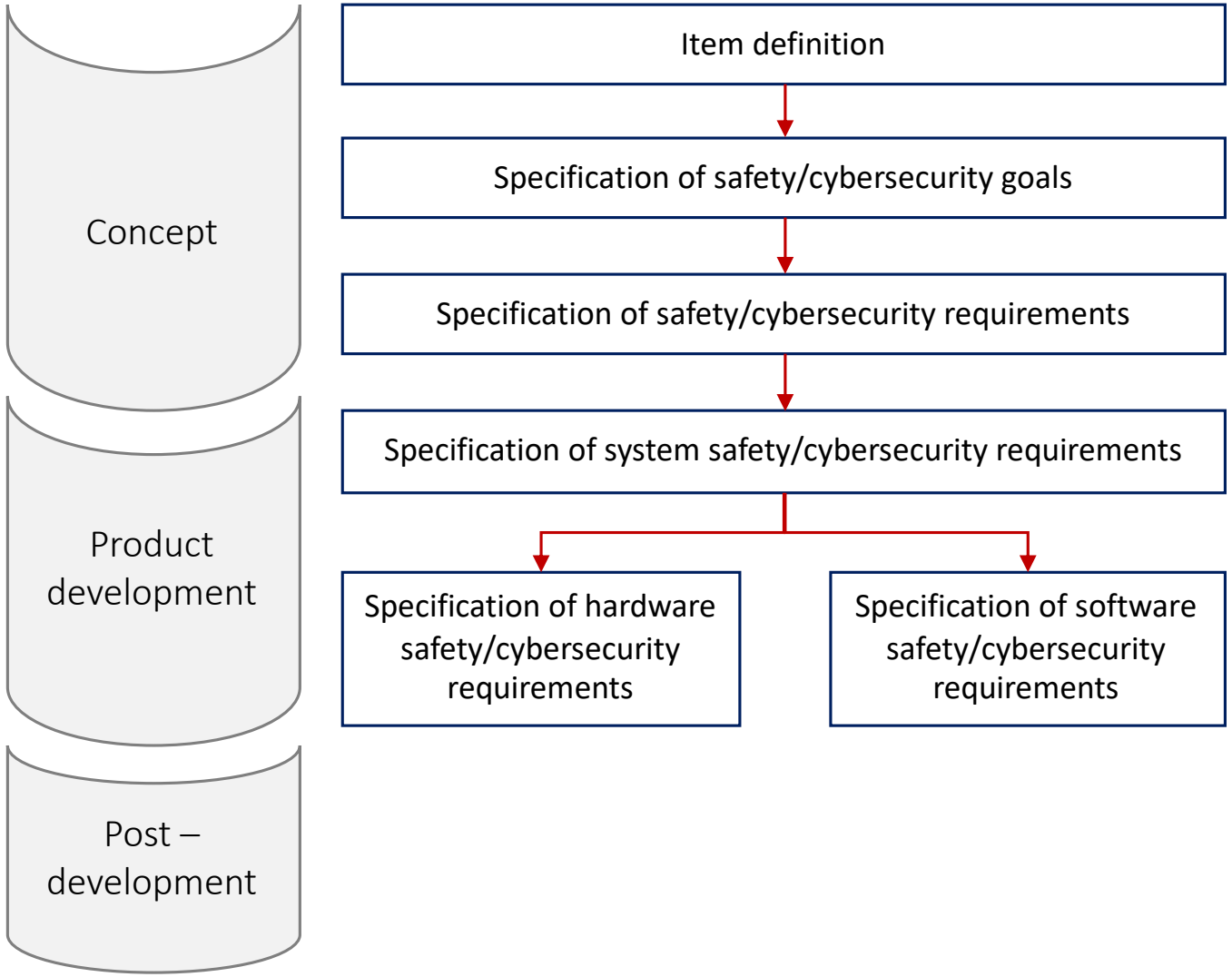
*** Learn About Quality. American Society for Quality (ASQ). 2019. https://asq.org/quality-resources/qfd-quality-function-deployment*

Example of Quality Function Deployment (QFD) matrices*



*Learn About Quality. American Society for Quality (ASQ). 2019. https://asq.org/quality-resources/qfd-quality-function-deployment

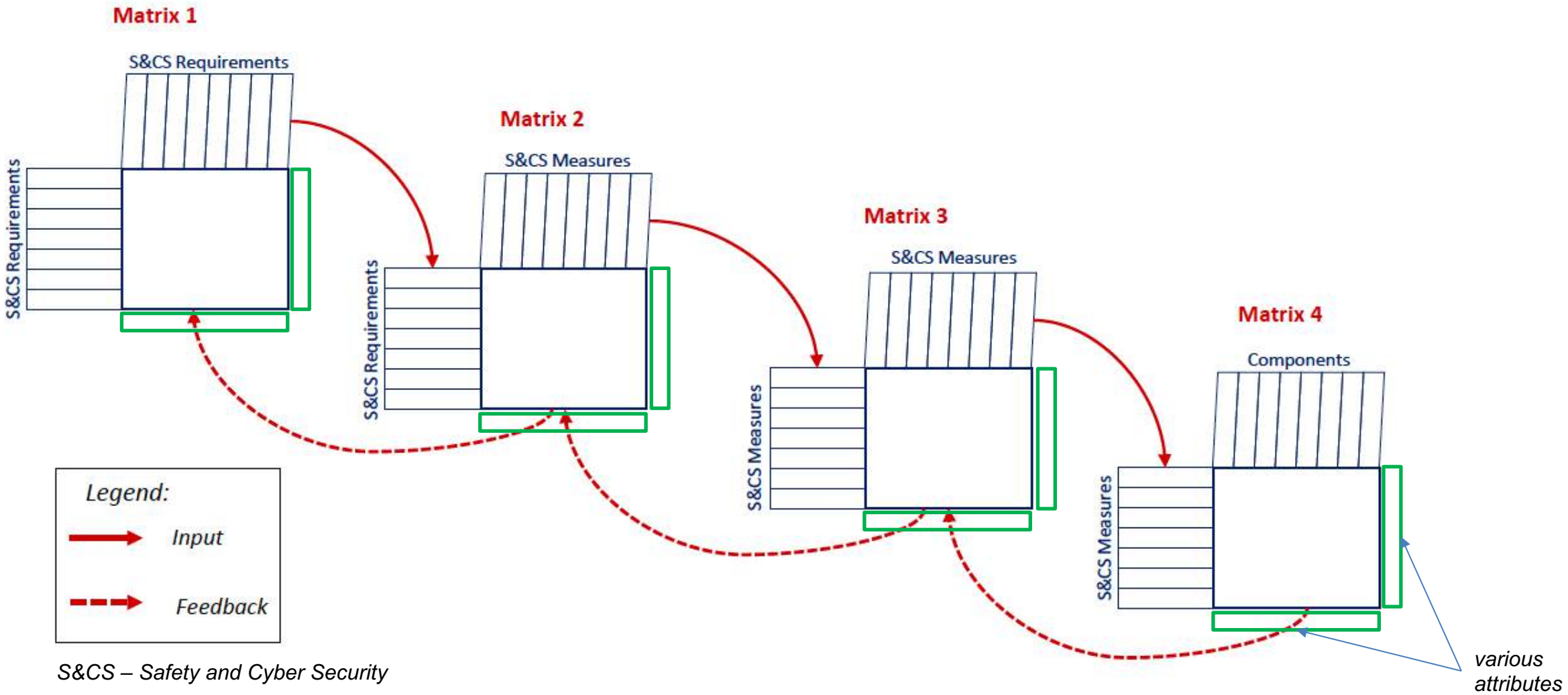
Compliance with international standards ISO 26262 (safety) and ISO/SAE 21434 (cybersecurity)



Safety requirement *= hazardous event (failure) + safety measure + allocation to system components*

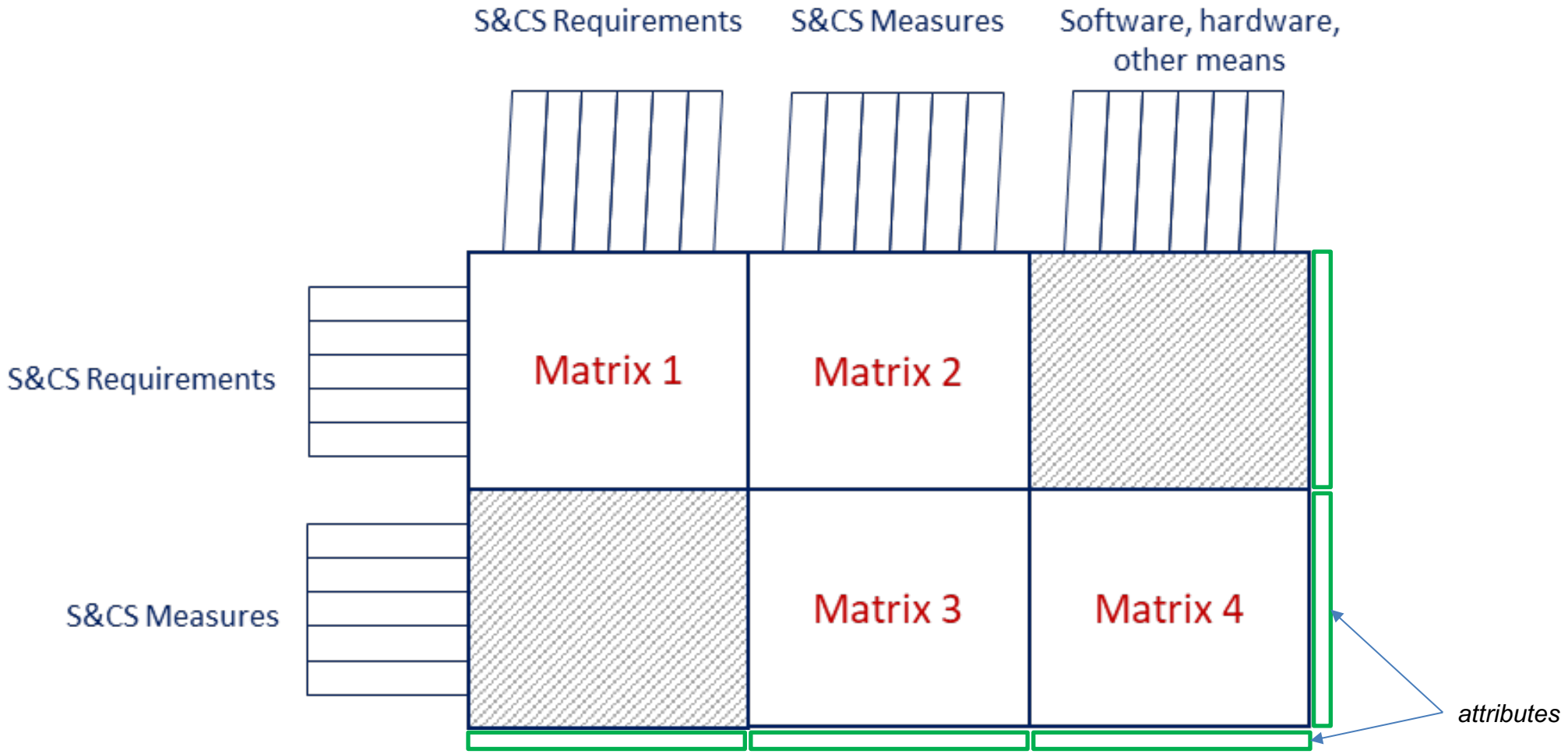
Cybersecurity requirement *= threat scenario (attack) + security measure + allocation to system components*

Four QFD-inspired matrices for analyzing safety and security inter-relationships*



*G. Sabaliauskaite, L. S. Liew, and F. Zhou. AVES - Automated Vehicle Safety and Security Analysis Framework. ACM Computer Science in Cars Symposium (CSCS 2019). 8 October 2019. Kaiserslautern, Germany.

Model 3: Safety and Cyber Security Deployment (SCSD) Model*

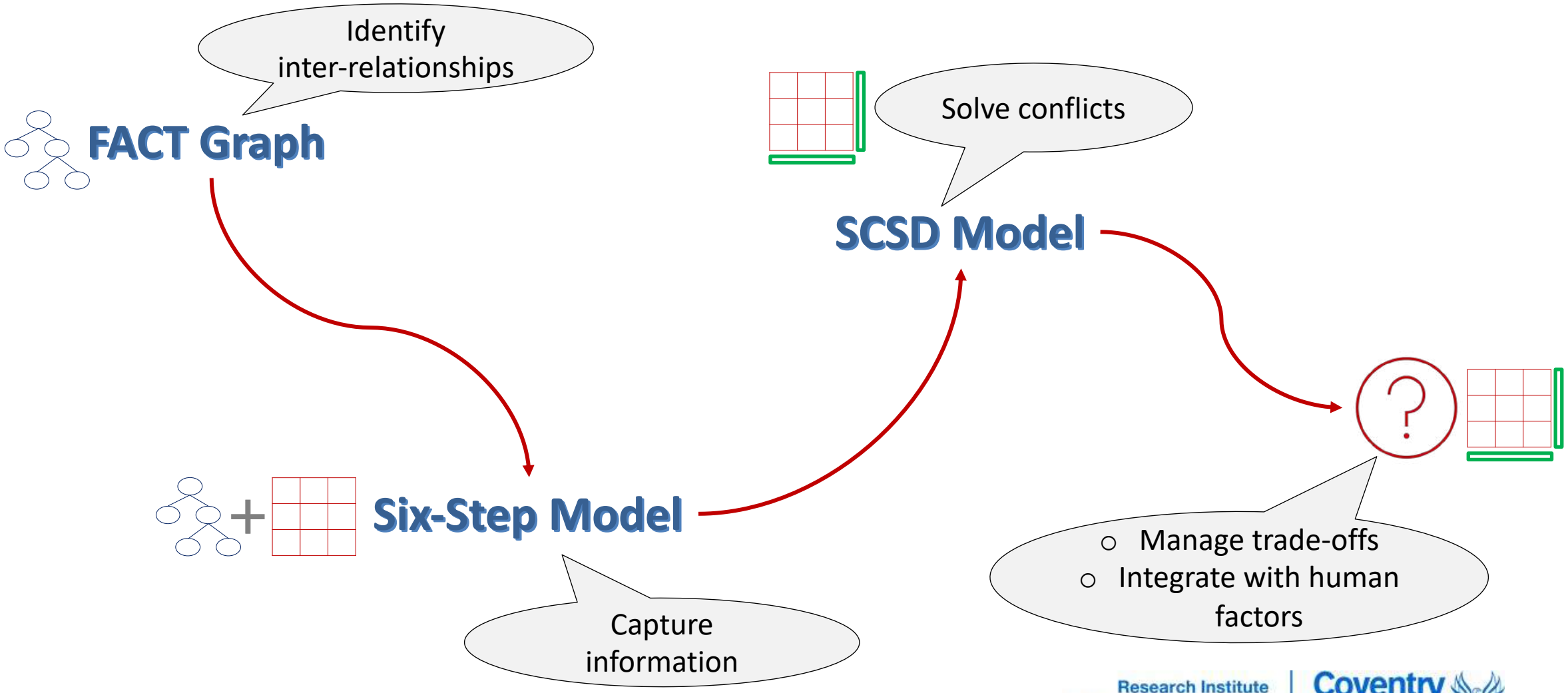


**G. Sabaliauskaite, L. S. Liew, and F. Zhou. AVES - Automated Vehicle Safety and Security Analysis Framework. ACM Computer Science in Cars Symposium (CSCS 2019). 8 October 2019. Kaiserslautern, Germany.*

Summary of proposed models

Photo by ThisisEngineering RAEng on Unsplash

Transition between FACT Graph, Six-Step Model, and SCSD Model



Challenges with integrated safety and security analysis methods

Recent survey on cyber-physical system safety and cybersecurity co-engineering reports on **sixty-eight methods**, which span a time period of around twenty years*

What is still missing? What are the main challenges?

- Compliance with safety and cybersecurity standards
- Independence of application domain
- Lack of quantitative approaches
- Lack of tool support
- Consideration of not only technical, but also socio-technical aspects
- Lack of guidance on resolving conflicts between safety and security

**G. Kavallieratos, S. Katsikas, and V. Gkioulos. Cybersecurity and Safety Co-Engineering of Cyberphysical Systems – A Comprehensive Survey. Future Internet. 2020; 12(4):65.*

Takeaways

“New is the well forgotten old”

When developing new methods or models

- Have their purpose very well defined
- Look for inspiration in methods used in other fields, for other purposes, developed long ago
- Think of compliance with international standards and tool support – this will help to implement them in practice
- Good luck!

Road trip with Raj photo on Unsplash

Thank you!

Giedre Sabaliauskaite

ad5315@coventry.ac.uk

Research Institute
Future Transport and Cities

Coventry University