intecs Solutions

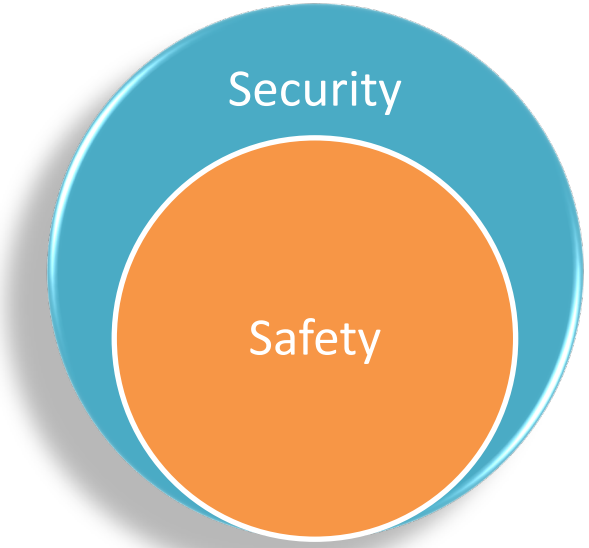
SYSTEM ENGINEERING
SOFTWARE DEVELOPMENT
PROCESS & RAMS CONSULTING
VALIDATION & VERIFICATION
EMBEDDED SOFTWARE

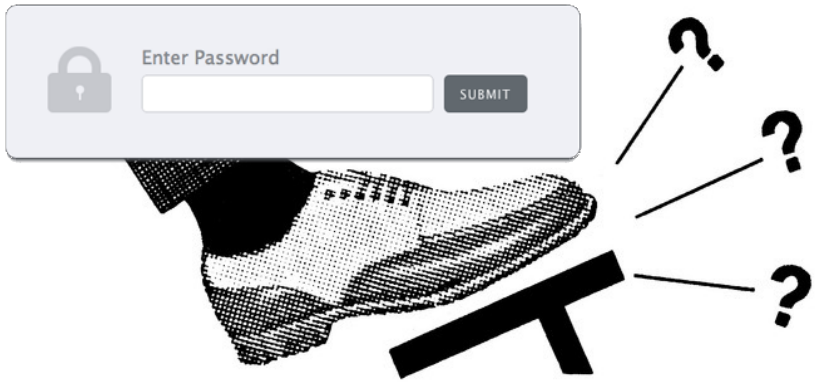
Automotive SPIN 2023
Challenges of the interactions between Safety and Security

Speaker: Rigels Gordani

Safety and Security

- Cyber-physical vehicle systems are **safety critical**
- Not all security related systems are safety critical
  - Privacy, confidentiality, financial (e.g., toll services)
  - Infotainment (although we will see that it is more complicated than it seems!)
- But all safety related systems are security critical
  - A security breach can lead to a safety related event
  - Placing a password on the braking system …
  - Even a tire pressure monitoring system revealing the location of a VIP for a terror attack



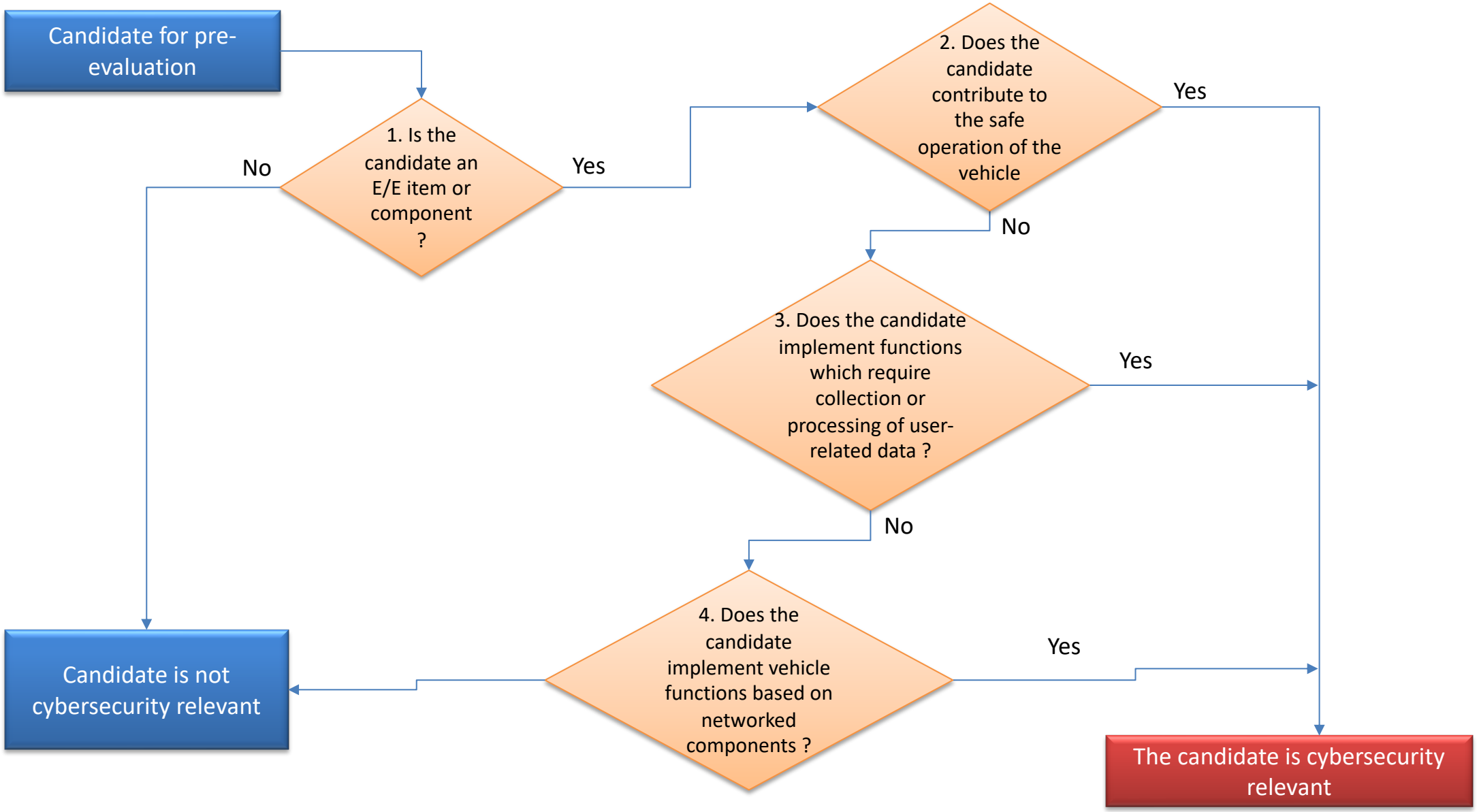


Some Comparative Statistics

- ISO 26262 is 12 documents with a total of more than 1000 pages
  - Part 11 *alone* has 188 pages
- There are more than 600 requirements
- There are more than 120 work products

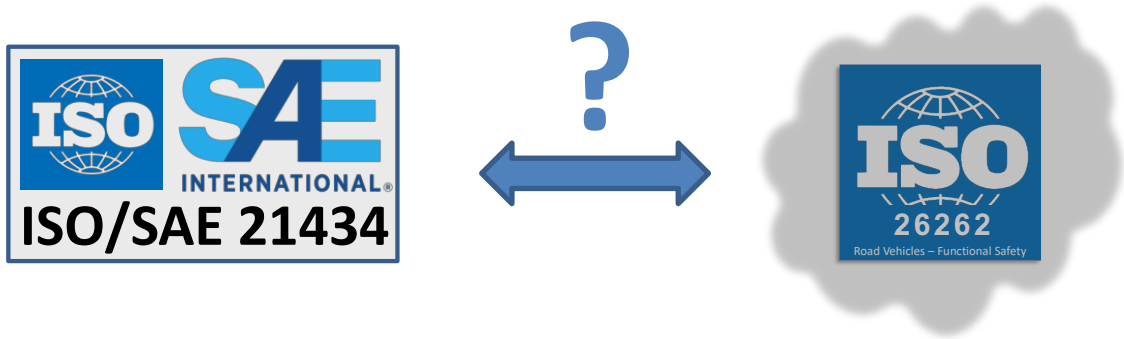
- The **entire** ISO/SAE 21434 Standard is a single document, with only 87 pages
  - Only the first 49 pages are normative
  - The other 38 pages are Informative Annexes
- There are approximately 117 requirements
- There are approximately 42 work products

Cybersecurity relevance ISO 21434



ISO/SAE 21434 versus ISO 26262

- Some considerations concerning the relative length of ISO/SAE 21434
  - Cybersecurity is less consolidated than safety
    - Risk assessment is still relatively controversial
  - ISO/SAE 21434 may **seem** short, but much is hidden inside
    - It often refers in one sentence to entire sections of other standards and says “Do it that way”
    - Examples: the supporting processes like configuration, change, requirements management
    - Examples: freedom to use trusted practices, trusted workflows, trusted life cycle models
  - Much is in informative appendices because agreement was not yet reached
    - Example: the Cybersecurity Assurance Level
- Overall, ISO/SAE 21434 is considered a **start** rather than a final statement on cybersecurity engineering



Comparison to ISO 26262

function(s)

malfunction
asset

attribute of

cybersecurity
property

road user

implements

protects against

compromises

affects

item

associated with

cybersecurity
goal

safety goal

associated with

threat
scenario

realizes

damage
scenario

hazard

harm

consists of

allocated to

realized by

Security is more
general than safety

component

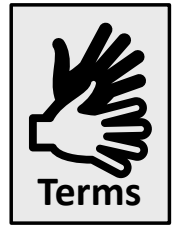
cybersecurity
requirement

functional safety requirement

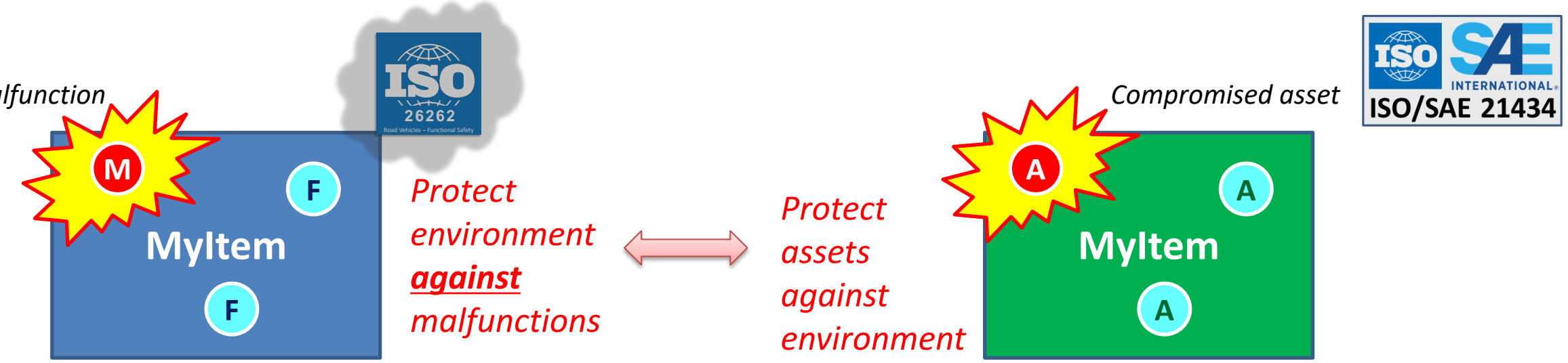
allocated to

*"Safety protects the environment against the system
Security protects the system against the environment"*

*The analogy is **imperfect**, but there is a clear attempt to remain conceptually aligned as much as possible*



Cybersecurity and Functional Safety Assets



*Identify **functionalities** of the item whereby compromising their properties of correctness (in other words, malfunctioning) could lead to **harm***

*Identify **assets** of the item whereby compromising their cybersecurity properties could lead to **damage scenarios***

The analogy isn't perfect: cybersecurity is broader, with more potential stakeholders. But in both cases, a qualitative, systematic, and usually iterative process must be followed to identify the functionalities / assets. They could be identified at many points over the life cycle.

Integrated Asset Identification!

Again and again, we stress that safety and cybersecurity should be integrated

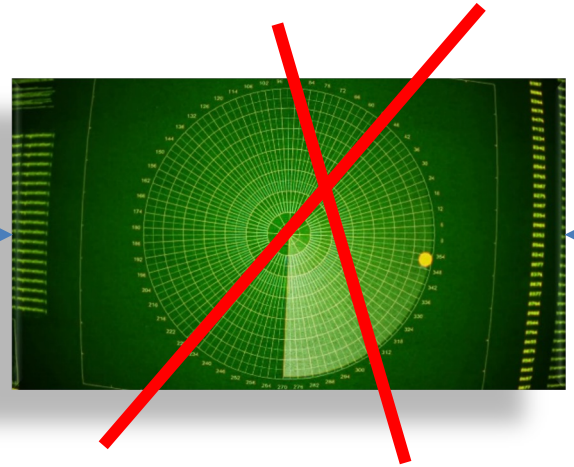
Partial knowledge is dangerous

Safety team

Safe State

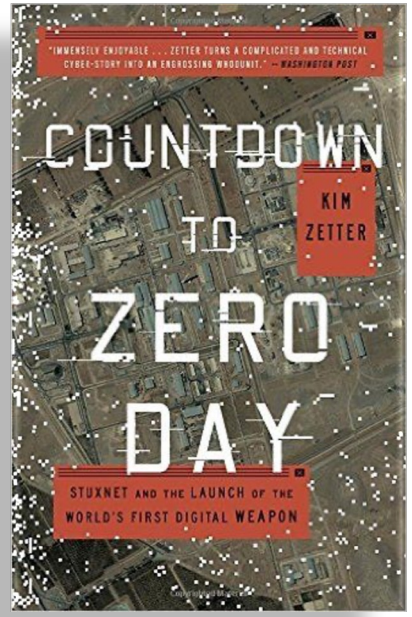
Security team

Low-Value



Attacks on protection mechanisms

Here is an example of a real insider attack: the security team had judged a particular element as low-value (not an "asset to protect"). But the safety team (and the insider!) knew it was critical to achieving the safe state.



Example 1

Introduction:

Safety team uses a dedicated hardware part with a software component in order to read peripheral data with very low delay. Cybersecurity team allows usage of the hardware part ONLY for debug usage not in production. But safety team and cybersecurity team do not have a well-established communication channel.

Problem:

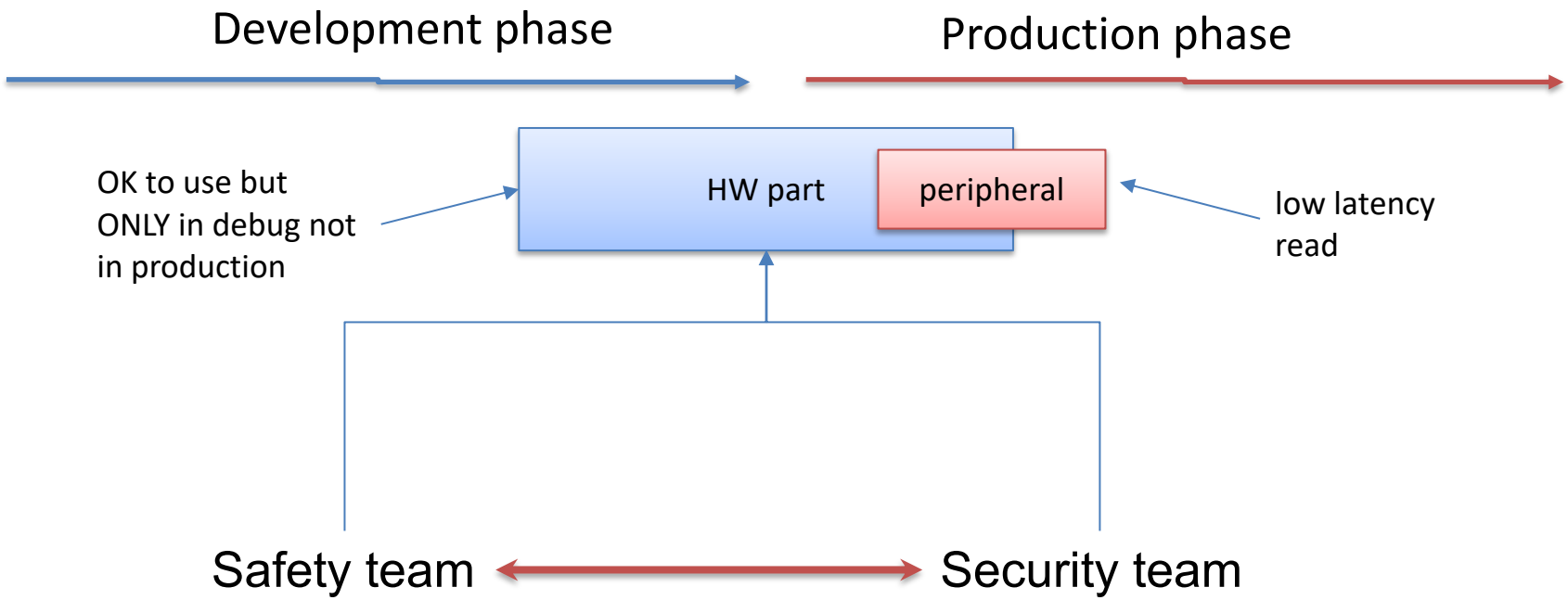
Safety team cannot use the hardware part in production thus not able to read the peripheral data with very low delay yielding unsatisfied customer requirements.

Solution:

Establish a well-defined defined communication channel between Safety and Cybersecurity teams. Make sure that the hardware part and the software component can be used in production and does not have limitation (e.g.,, can be used only for debugging)

well-established: means that it has been **in existence for quite a long time and is successful.**

Example 1



Safety team and cybersecurity team do not have a well-established communication channel.

Example 2

Example 2

Introduction:

Functional Safety team uses SHA-1 algorithm to protect the integrity of large data buffer (<= 1MB) elaborated by the infotainment ECU, that is exchange between two safety relate software components.

Problem:

SHA-1, short for Secure Hash Algorithm 1, is a 27-year-old hash function used in cryptography and has since been deemed broken owing to the risk of collision attacks. Thus, SHA-1 has security problems and is not accepted by cybersecurity team*.

Solution:

Establish a well-defined defined communication channel between Safety and Cybersecurity teams. Make sure that the algorithms used by safety team are the state-of-art regarding security aspects. Perform, frequent trainings for safety and cybersecurity teams.

*https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm

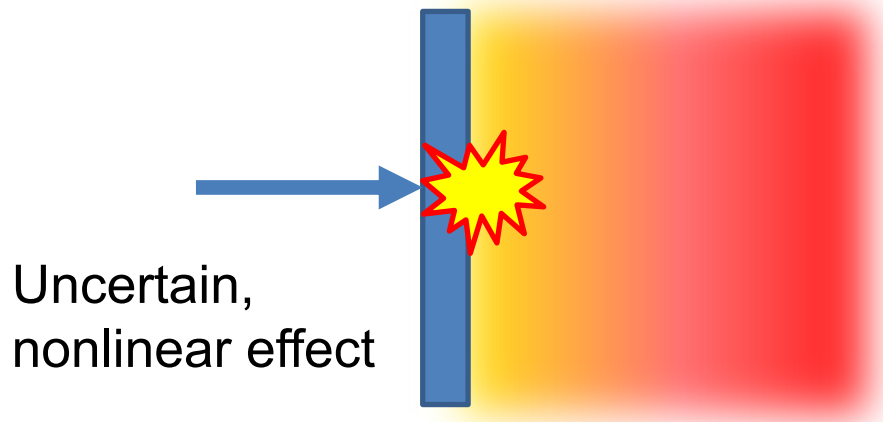
How Requirements Conflict

- One of the most important tasks of interaction among disciplines is to resolve conflicting requirements (such as whether to connect two internal buses!)
- Safety requirements are much simpler
  - E.g., “Avoid hazards / accidents”
  - At a high level, they are generally quite obvious
- Security requirements can be much more complex
  - For example, they could also involve **privacy**
  - Safety experts don’t care if the Tire Pressure Monitoring system is broadcasting data – but both security and privacy experts might protest strongly!

TPMS

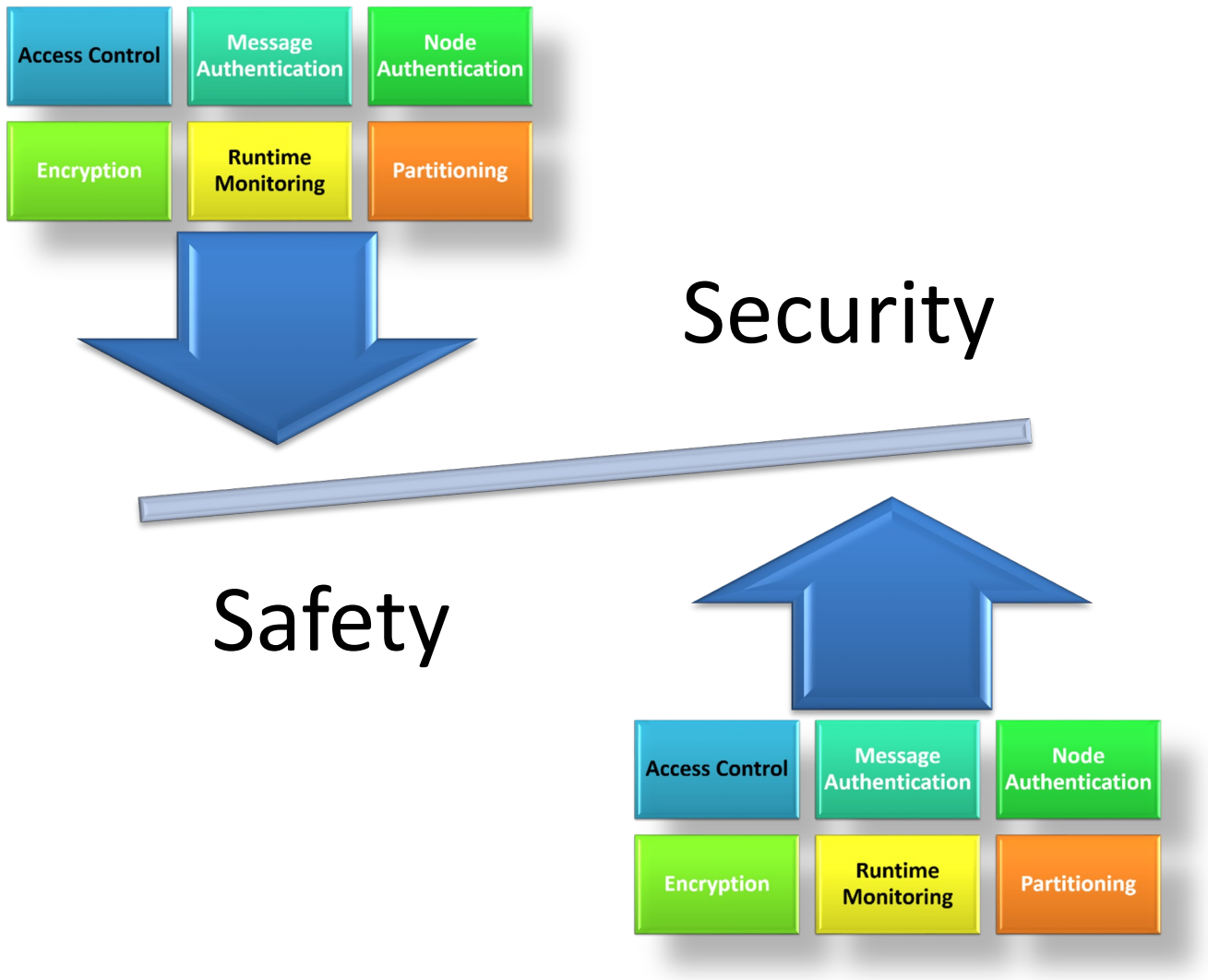
Non-linear cybersecurity risk

- In cybersecurity, the penetration of one single vulnerable element of the system could open up the entire system, making the risk explode
- Because it makes it possible to attack components that **do not even depend on the compromised component**



Dynamic, Malicious

Architecture: Safety Versus Security



A typical trade-off analysis takes place with the integrated development of both the safety and security architecture from building blocks.

SYSTEM ENGINEERING
SOFTWARE DEVELOPMENT
PROCESS & RAMS CONSULTING
VALIDATION & VERIFICATION
EMBEDDED SOFTWARE

Special thanks to John Favaro and Ferdinando Bultrini

Intecs Solutions S.p.A
Via Umberto Forti, 5 Loc. Montacchiello
56121 Ospedaletto - Pisa
Phone: +39 050 96 57 507

www.intecs.it