RI.
SE

11TH SCANDINAVIAN CONFERENCE ON SYSTEM & SOFTWARE SAFETY – STOCKHOLM – BEHROOZ SANGCHOOLIE

# Analyses of the interplay between safety and security attributes in connected computer systems

# Agenda

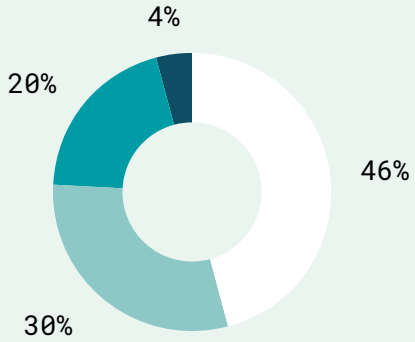
# Analyses of the interplay between safety and security attributes in connected computer systems

# 3,993

**SEK million, net sales**

Operating results: 22 SEK million

Operating margin: 0,6%




## Distribution of net sales

| | |
|---|---|
| Business sector | 1,831 MSEK |
| Public funds | 1,179 MSEK |
| State funds | 812 MSEK |
| EU funds | 171 MSEK |

Nearly

# 3,300

**employees**


We are represented at

# 35

locations around Sweden

# 130+

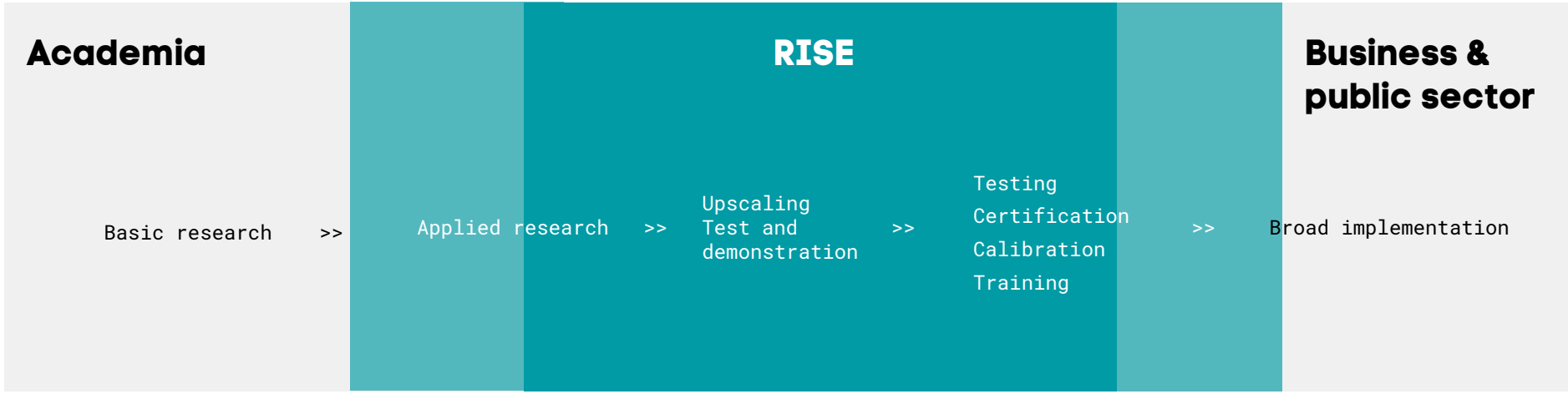
**Testbeds and demonstration environments**

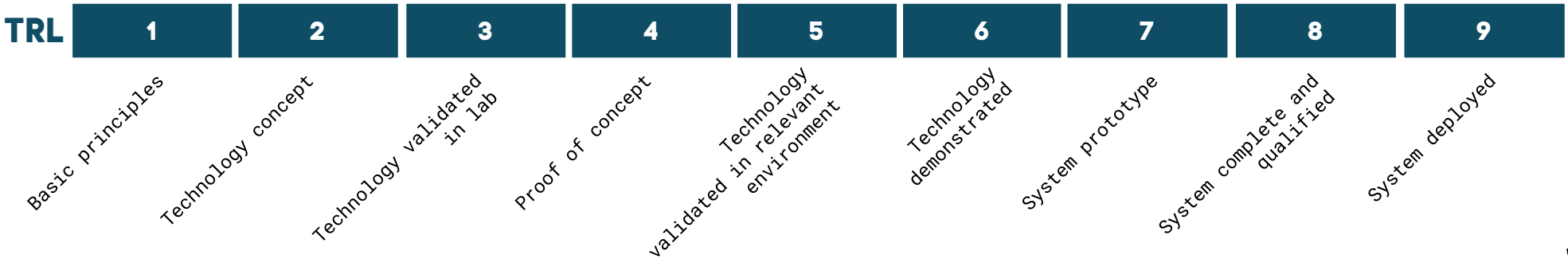
# 78

**Customer Satisfaction Index**

Alla siffror avser 2022.

# RISE in the innovation value chain

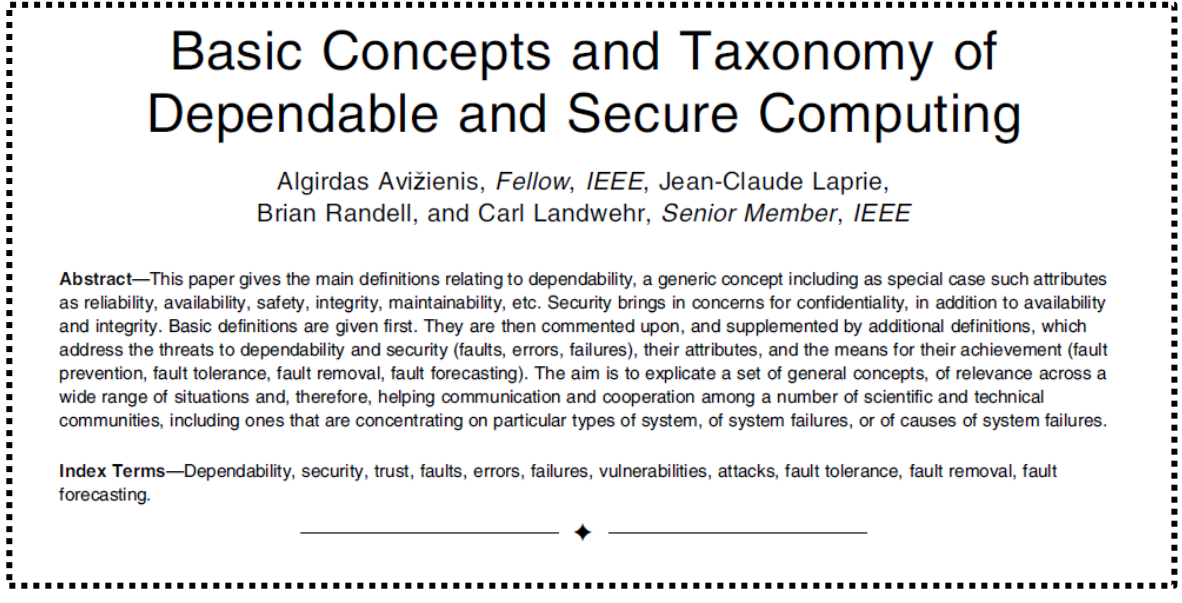


# Agenda

# Analyses of the interplay between safety and security attributes in connected computer systems

# Dependability and security attributes*



Basic Concepts and Taxonomy of Dependable and Secure Computing

Algirdas Avižienis, *Fellow*, *IEEE*, Jean-Claude Laprie,
Brian Randell, and Carl Landwehr, *Senior Member*, *IEEE*

**Abstract**—This paper gives the main definitions relating to dependability, a generic concept including as special case such attributes as reliability, availability, safety, integrity, maintainability, etc. Security brings in concerns for confidentiality, in addition to availability and integrity. Basic definitions are given first. They are then commented upon, and supplemented by additional definitions, which address the threats to dependability and security (faults, errors, failures), their attributes, and the means for their achievement (fault prevention, fault tolerance, fault removal, fault forecasting). The aim is to explicate a set of general concepts, of relevance across a wide range of situations and, therefore, helping communication and cooperation among a number of scientific and technical communities, including ones that are concentrating on particular types of system, of system failures, or of causes of system failures.

**Index Terms**—Dependability, security, trust, faults, errors, failures, vulnerabilities, attacks, fault tolerance, fault removal, fault forecasting.

Cited in over 7000 papers.

* A. Avizienis, J. . -C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-March 2004, doi: 10.1109/TDSC.2004.2.

# Dependability attributes*

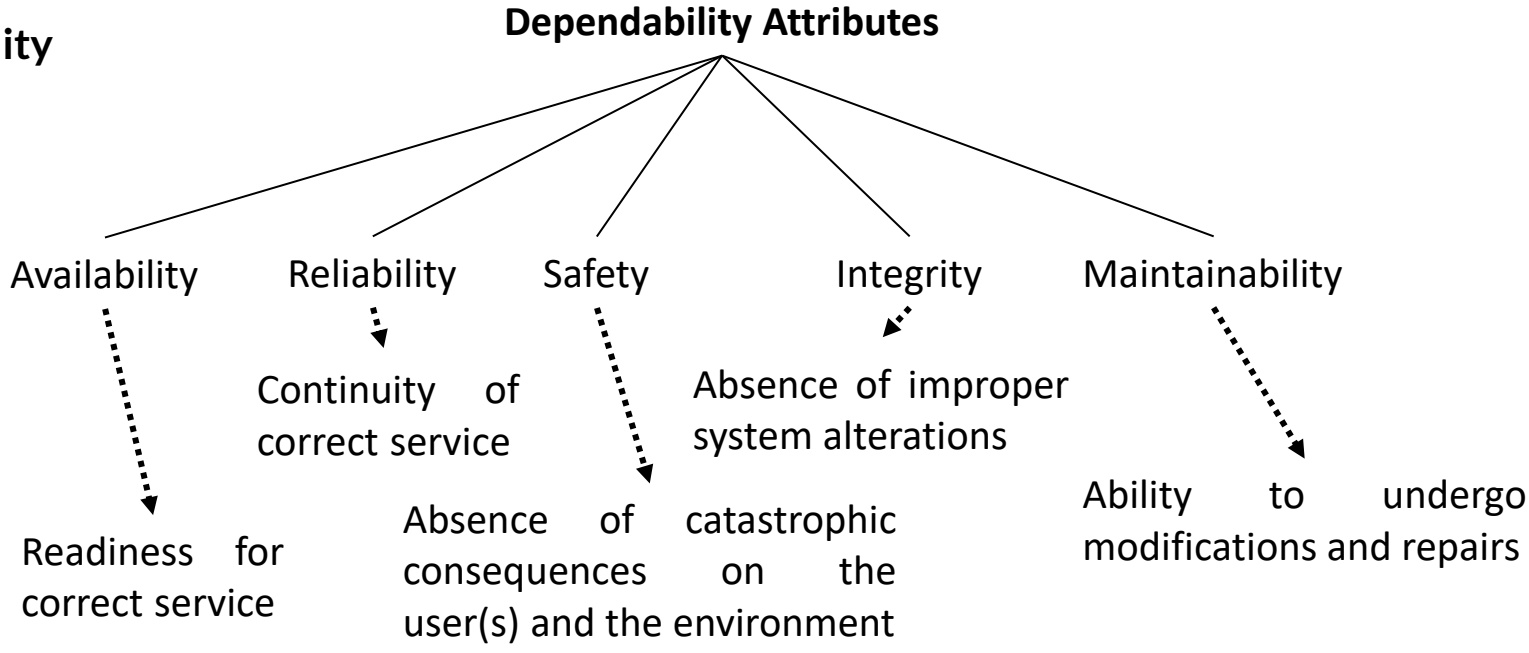
**Other dependability attributes:**

Maintainability

Integrity

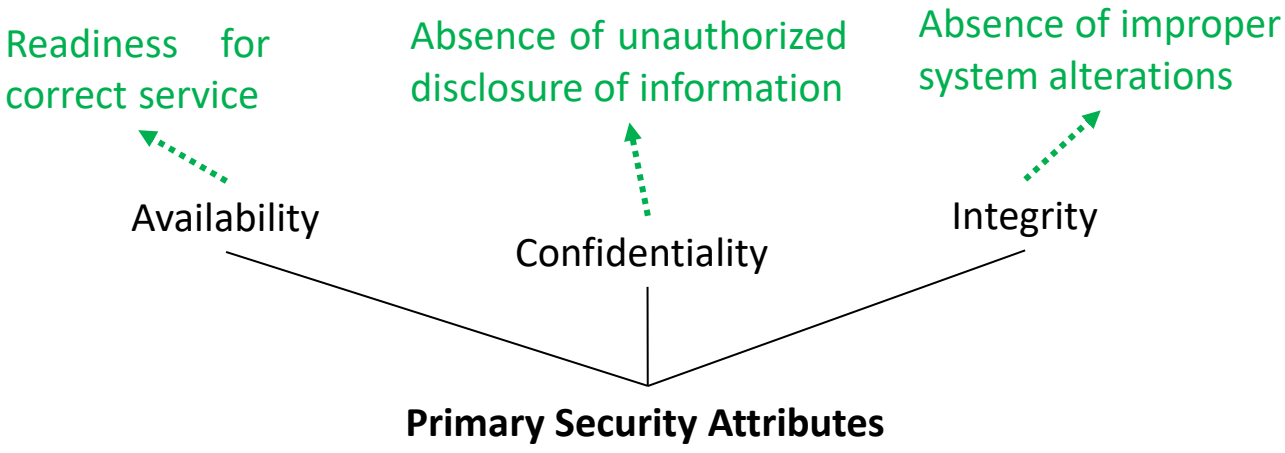
Reliability

Availability



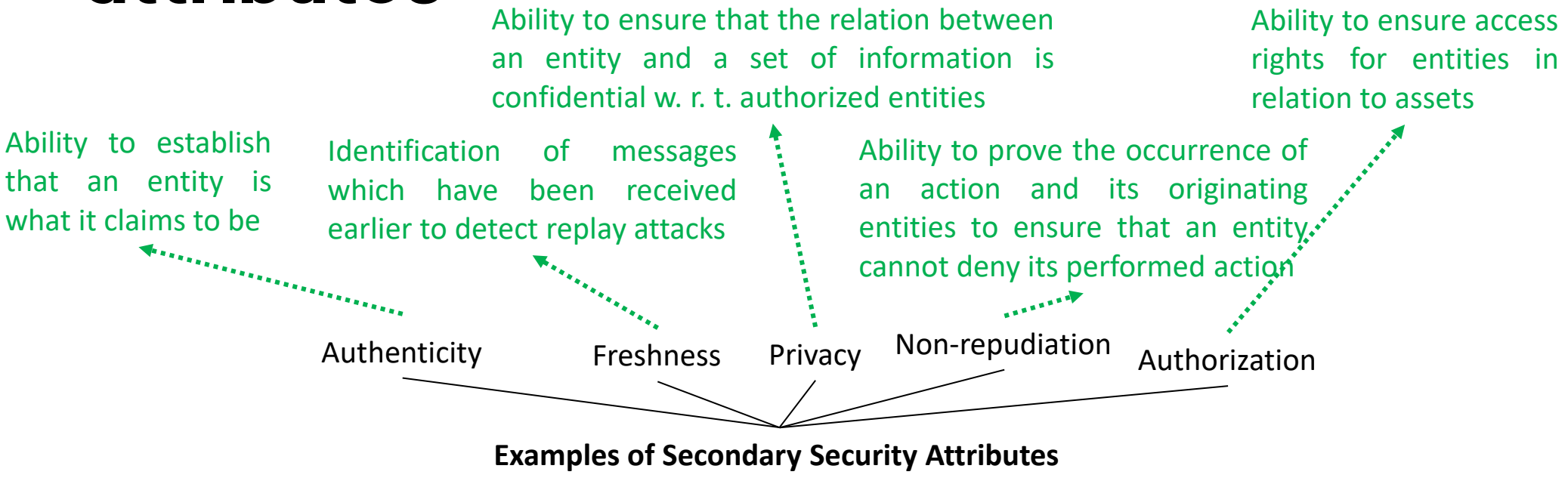

* A. Avizienis, J. . -C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-March 2004, doi: 10.1109/TDSC.2004.2.

# Primary security attributes *




* A. Avizienis, J. . -C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-March 2004, doi: 10.1109/TDSC.2004.2.

# Examples of secondary security attributes*




**Examples of Secondary Security Attributes**

* A. Lautenbach et al. Deliverable d2.0, security models, heavens (healing vulnerabilities to enhance software security and safety). Technical report, HEAVENS project, 2016.

# Agenda

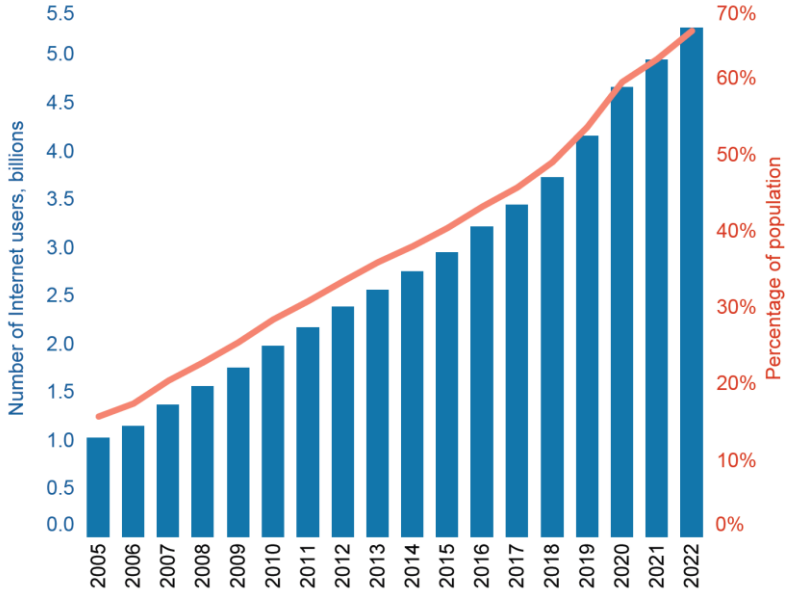
# Analyses of the interplay between safety and security attributes in connected computer systems

# ”The ability of a computer, program, device, or system to connect with one or more others”

**Definition of Connectivity according to the Cambridge Dictionary**

# Era of Connectivity

## Individuals using the Internet




International telecommunication union (ITU*) - Measuring digital development: Facts and figures 2022
** The UN specialized agency for ICTs*

## Universality targets: Achieving universal, affordable, connectivity by 2030

**100%** of population aged 15+ uses the Internet

**100%** of households have Internet access

**100%** of businesses use the Internet

**100%** of schools are connected to the Internet

**100%** of population is covered by a mobile network of the latest technology[1]

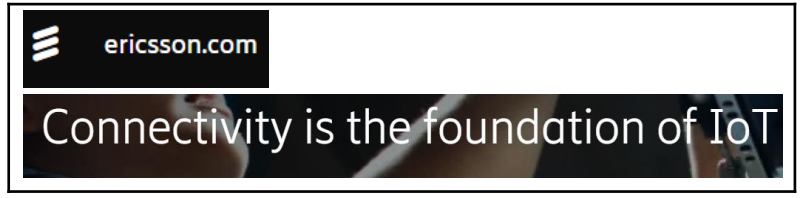
**100%** of population aged 15+ owns a mobile phone

The UN Secretary-General's Roadmap for Digital Cooperation

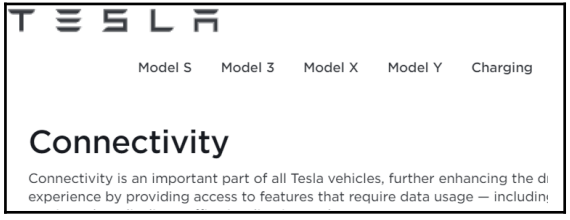
# Era of Connectivity














# Era of Connectivity






Increasingly digitalised, connected and personalized

Ensure safety and security

# Agenda

# Analyses of the interplay between safety and security attributes in connected computer systems

# ”The way in which two or more things or people affect each other”

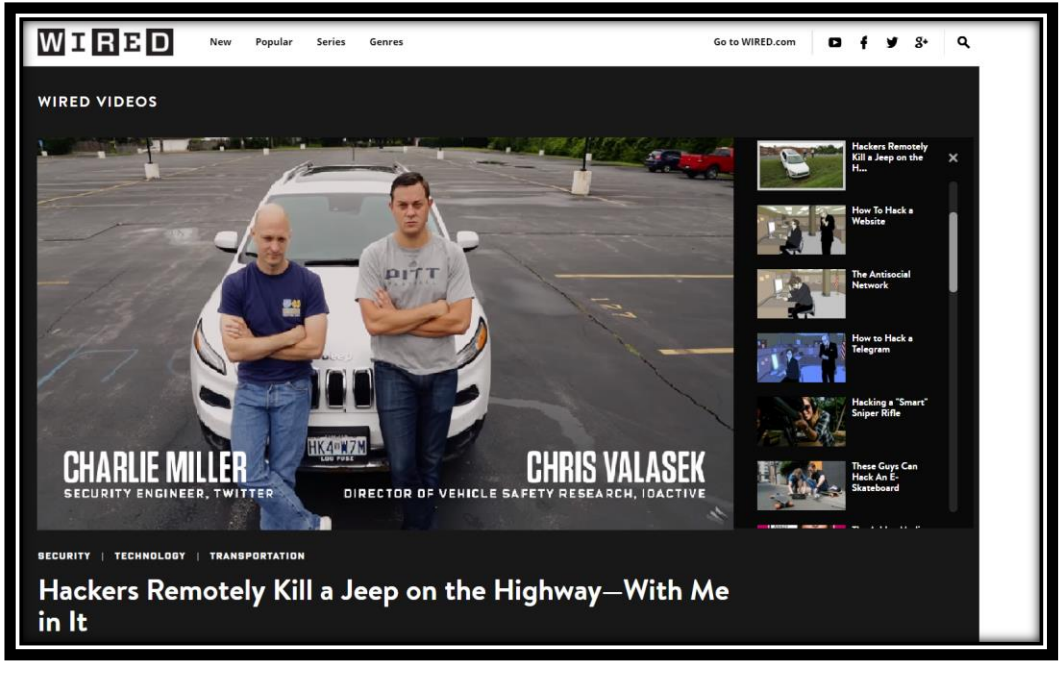
**Definition of Interplay according to the Oxford Dictionary**

# The way in which the means to obtain dependability and security affect each other

**Interplay between dependability and security**

# Interplay between safety and security

- An example from 2015 (Wired).



# Interplay between safety and security

- An example from 2016 (BBC).

# Interplay between safety and security

- An example from 2016 (The Gardian).

Team of hackers take remote control of Tesla Model S from 12 miles away

**Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc**



▲ Now that cars such as Tesla's are increasingly high-tech and connected to the internet, cybersecurity has become as big an issue as traditional safety features. Photograph: Jim Dyson/Getty Images

# Interplay between safety and security

- An example from 2020 (Associated Press).

## German hospital hacked, patient taken to another city dies

September 17, 2020

Click to copy

RELATED TOPICS

Europe
Technology
Hacking

BERLIN (AP) — German authorities said Thursday that an apparently misdirected ransomware attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment.

The woman's death appeared to be the first resulting from a ransomware attack, even if indirectly so.

The Duesseldorf University Clinic's systems have been disrupted for a week. The hospital said investigators have found that the source of the problem was a hacker attack on a weak spot in "widely used commercial add-on software," which it didn't identify.

As a consequence, systems gradually crashed and the hospital wasn't able to access data; emergency patients were taken elsewhere and operations postponed.

# Interplay between safety and security

- An example from 2021 (Wired).

## A Hacker Tried to Poison a Florida City's Water Supply, Officials Say

The attacker upped sodium hydroxide levels in the Oldsmar, Florida, water supply to extremely dangerous levels.

# Agenda

## Analyses of the interplay between safety and security attributes in connected computer systems

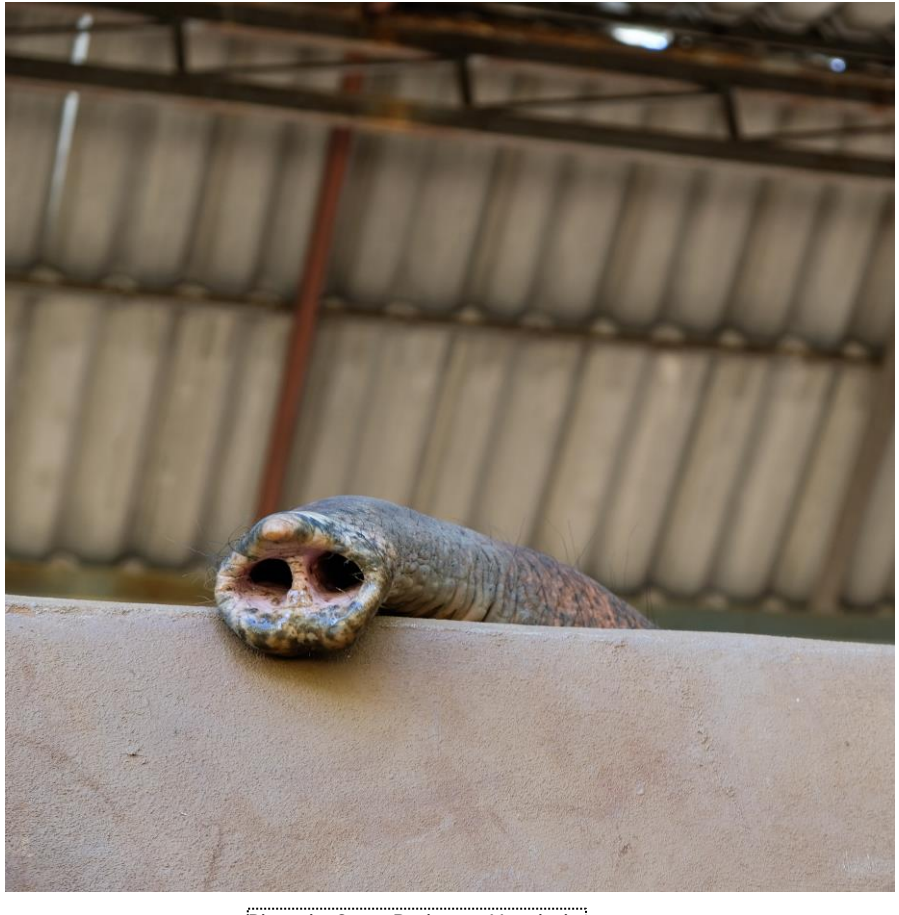
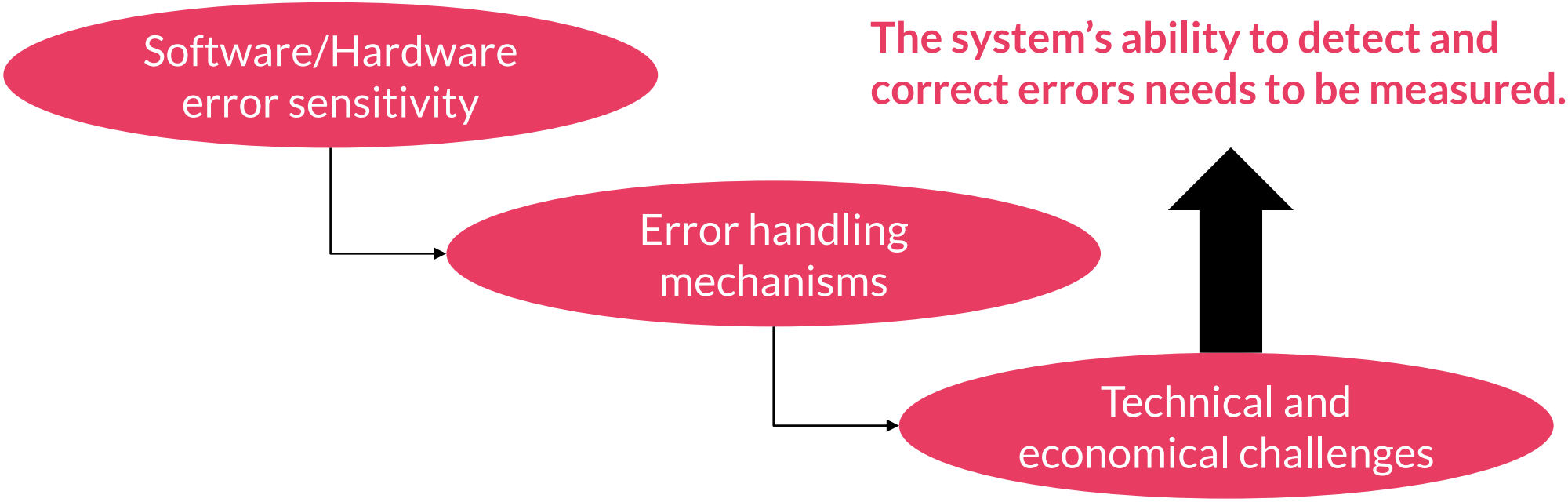


Photo by Steve Barker on Unsplash

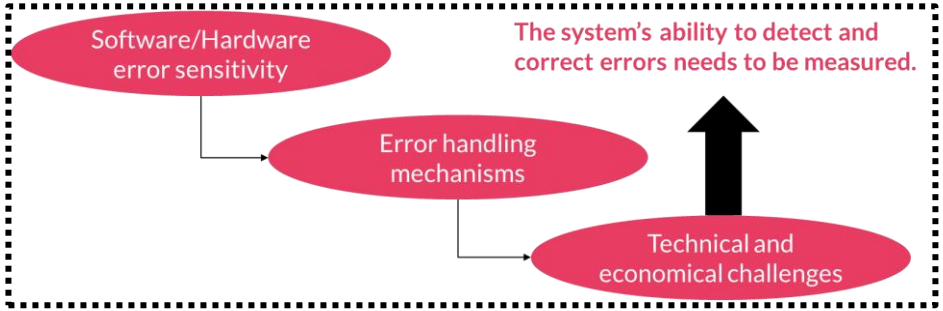
# Fault and Attack Injection to assess systems' safety and security

# Fault injection

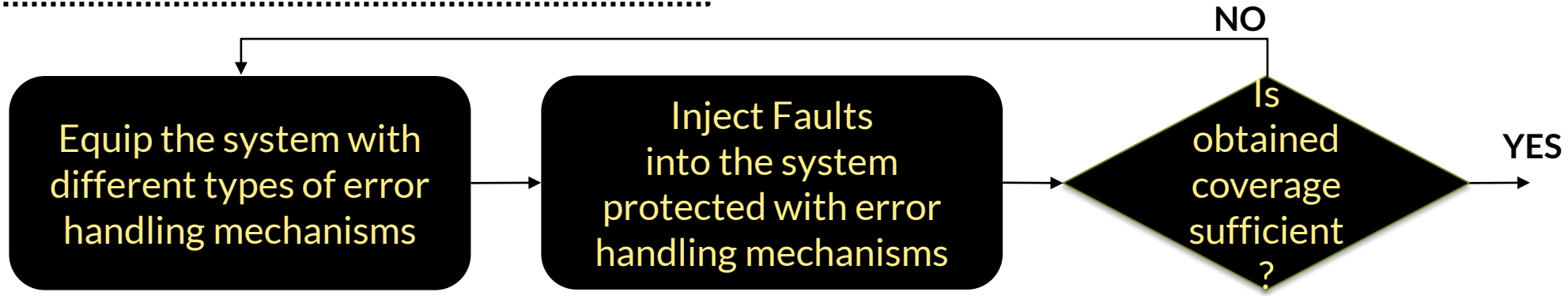



**The system's ability to detect and correct errors needs to be measured.**

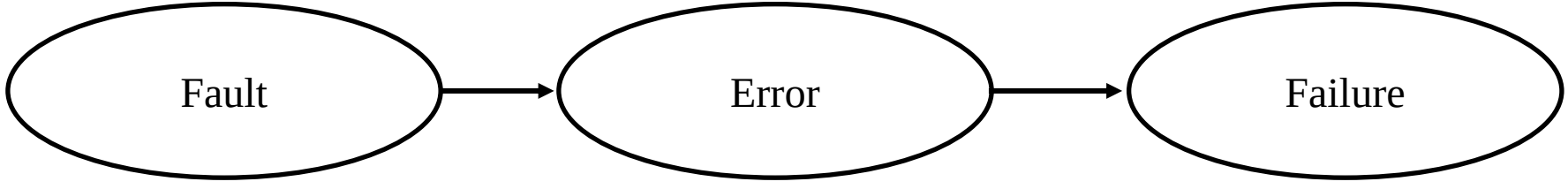
# Fault injection




**Fault injection has been effectively used to evaluate the effectiveness of safety mechanisms in the presence of different types of faults.**



# Threats to Dependability and Security*

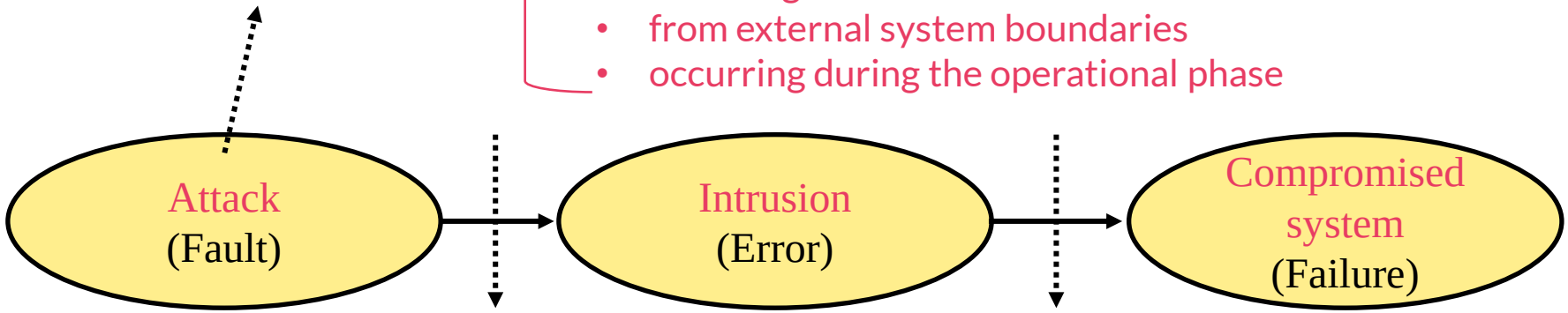



* A. Avizienis, J. . -C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-March 2004, doi: 10.1109/TDSC.2004.2.

# Threats to Dependability and Security*

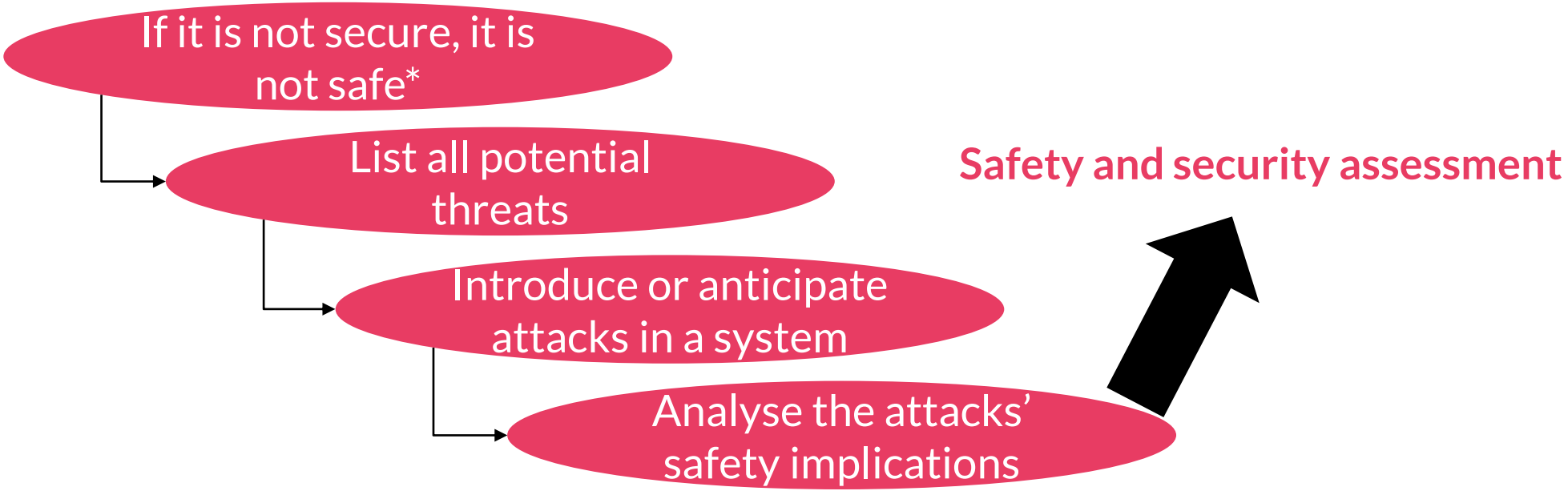
Attack is a special type of fault

- human made
- deliberate and malicious
- Affecting hardware/software
- from external system boundaries
- occurring during the operational phase




* A. Avizienis, J. . -C. Laprie, B. Randell and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," in IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-March 2004, doi: 10.1109/TDSC.2004.2.

# Fault and attack injection




* Bloomfield, R., Netkachova, K., Stroud, R. (2013). Security-Informed Safety: If It's Not Secure, It's Not Safe. In: Gorbenko, A., Romanovsky, A., Kharchenko, V. (eds) Software Engineering for Resilient Systems. SERENE 2013. Lecture Notes in Computer Science, vol 8166. Springer, Berlin.

# Analyses of the interplay between safety and security

Example-1

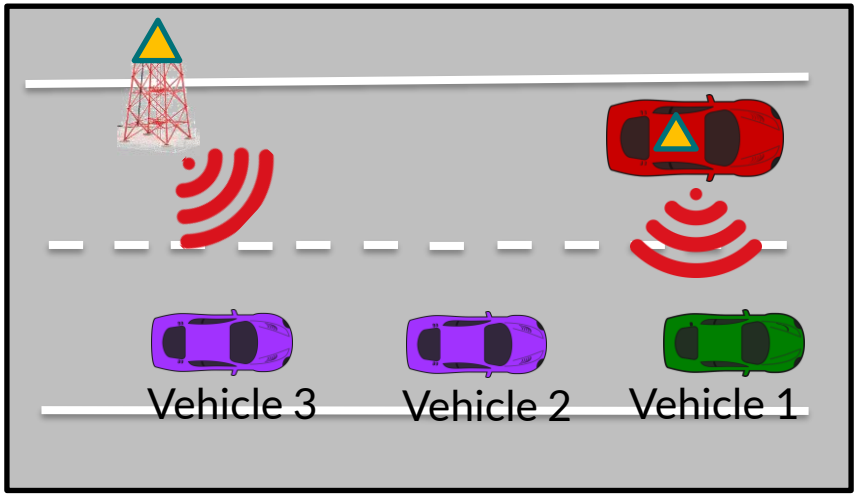
## Communication-based fault and attack injection (ComFASE)

M. Malik, M. Maleki, P. Folkesson, B. Sangchoolie and J. Karlsson, "ComFASE: A Tool for Evaluating the Effects of V2V Communication Faults and Attacks on Automated Vehicles," 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).

M. Maleki, M. Malik, P. Folkesson, B. Sangchoolie and J. Karlsson, "Modeling and Evaluating the Effects of Jamming Attacks on Connected Automated Road Vehicles," 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC).

M. Malik, M. Aramrattana, M. Maleki, P. Folkesson, B. Sangchoolie and J. Karlsson, "Simulation-based Evaluation of a Remotely Operated Road Vehicle under Transmission Delays and Denial-of-Service Attacks," 2023 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC).

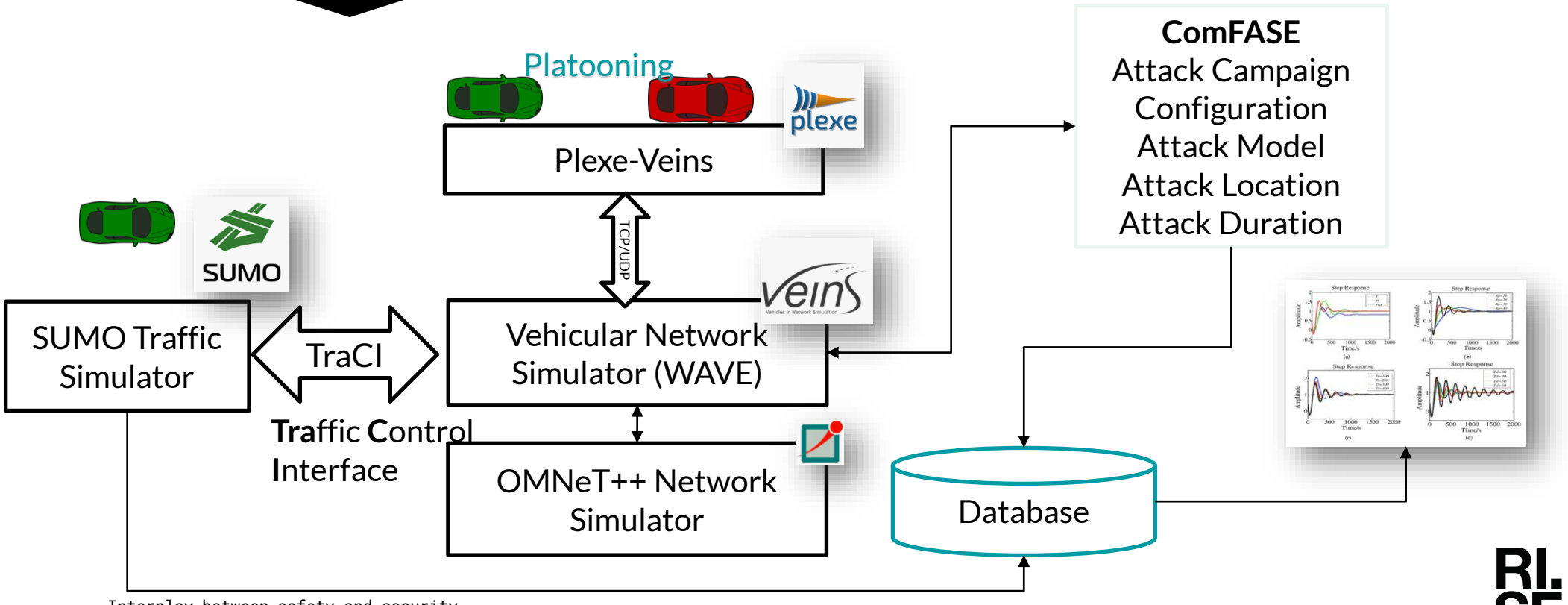
# System under test



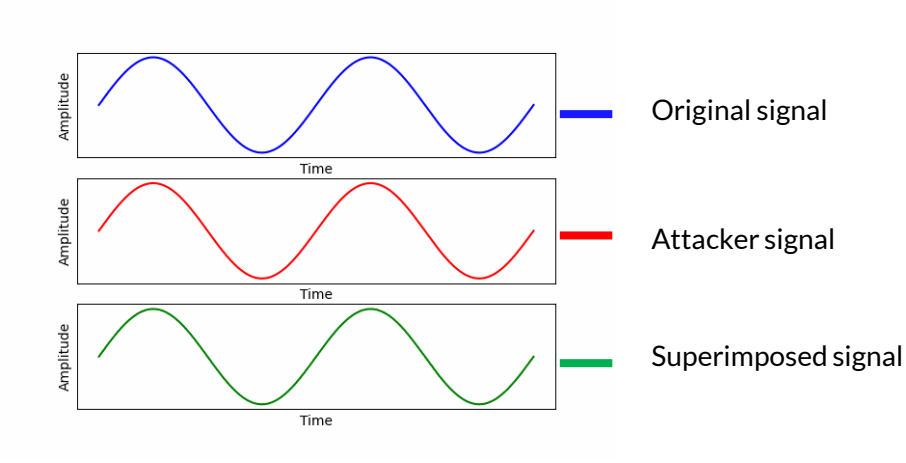

Platoon of vehicles
[discussed in the next slide]

Teleoperation

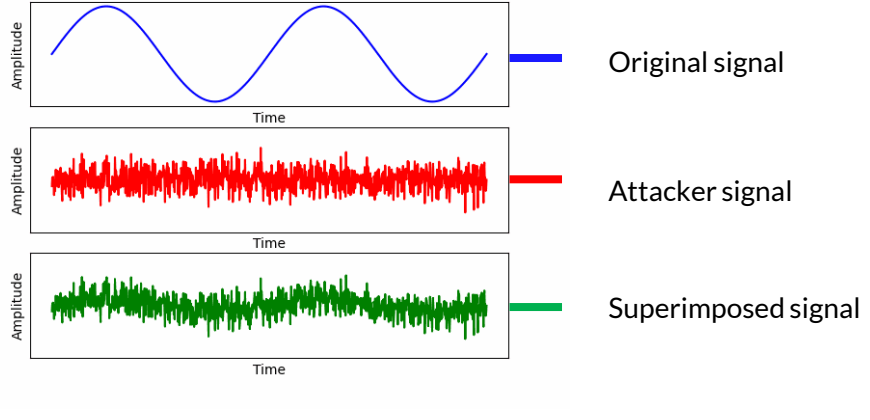
# Assessment method and tool



# Sample attacks

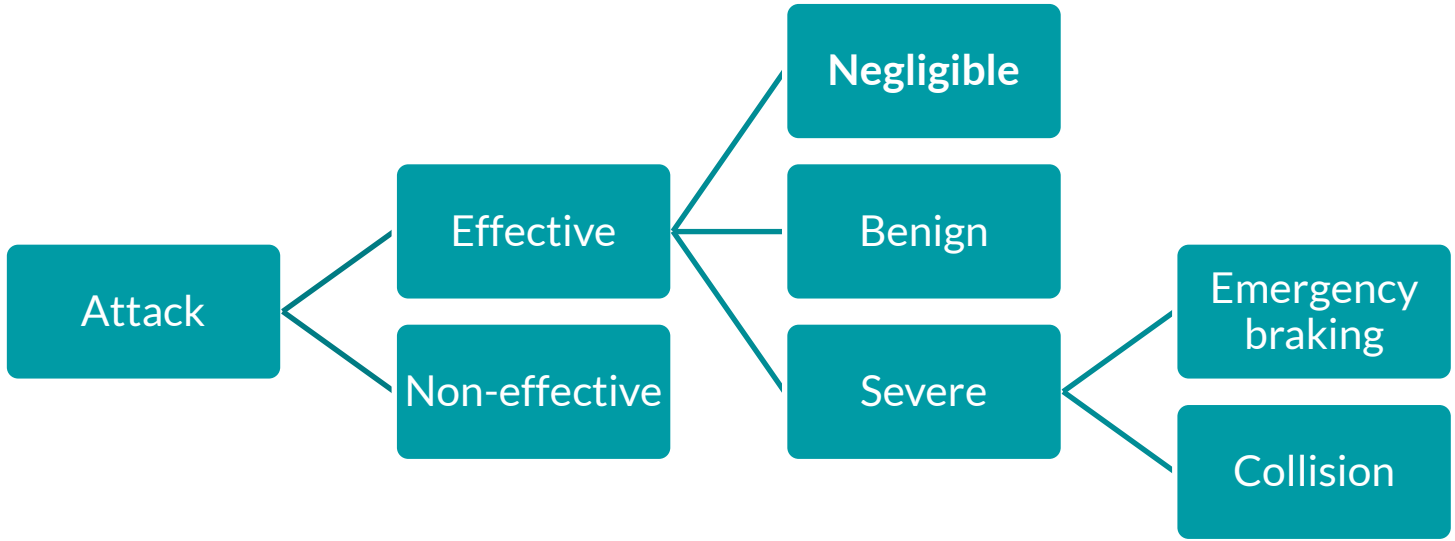



Destructive interference



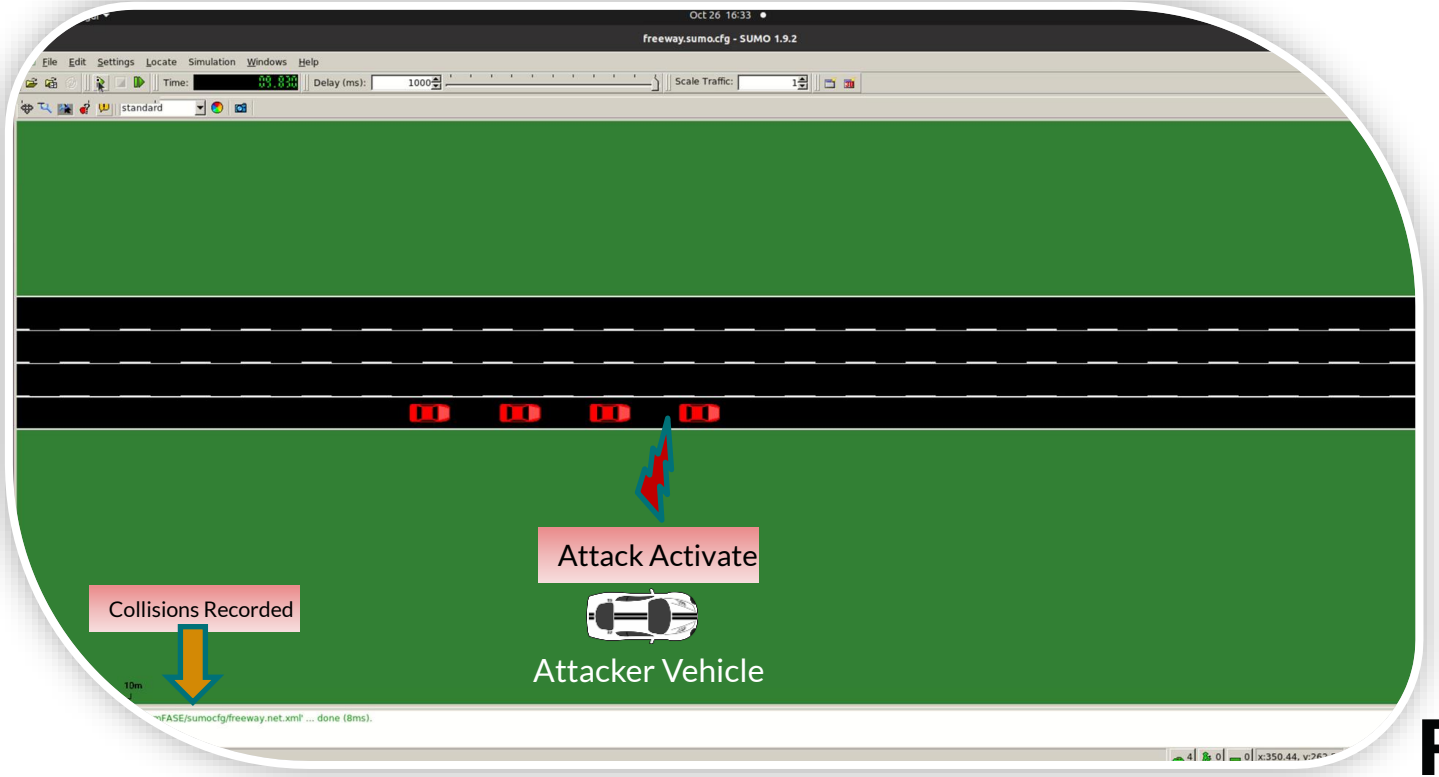

Barrage jamming

# Outcome classification



# Impact of an attack

Attack Type: Barrage Jamming
Attack Start Time: 17.2
Target Vehicle: all
Vehicles Speed: 100 km/h
Attack Value: **0.4mW**
Attack Duration: **5 seconds**



# Analyses of the interplay between safety and security

Example-2

## Cybersecurity mechanisms

B. Sangchoolie, P. Folkesson, P. Kleberger and J. Vinter, "Analysis of Cybersecurity Mechanisms with respect to Dependability and Security Attributes," 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), Valencia, Spain, 2020, pp. 94-101, doi: 10.1109/DSN-W50199.2020.00027.

# Security mechanisms*

| Mechanism | Prevention | Detection | Handling |
|---|---|---|---|
| access control | ✓ | | |
| authentication control | ✓ | | |
| device authentication | ✓ | | |
| firewalls | ✓ | | |
| virtual network | ✓ | | |
| encryption | ✓ | | |
| virtual private network | ✓ | | |
| log auditing | | ✓ | |
| intrusion detection/prevention systems | | ✓ | ✓ |
| virus/malicious code detection systems | | ✓ | ✓ |
| vulnerability scanning | ✓ | | |
| Host Configuration Management (HCM) and Automated Software Management (ACM) tools | | | ✓ |
| operating systems | ✓ | ✓ | ✓ |
| web technologies | ✓ | | |
| physical security controls | ✓ | | |
| signatures | ✓ | ✓ | |
| partitioning and separation | ✓ | | |

* Discussed in: IEC 62443, SESAMO, OWASP, NIST SP 800-53

# Impact of Cybersecurity Mechanisms on Dependability and Security Attributes

| | |
|---|---|
| High (positive) | ++ |
| Medium (positive) | + |
| Negligible | N |
| Negative | - |

| | | Dependability Attributes | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Primary Sec. Attr. | | | Secondary Sec. Attr. | | | | |
| **Mechanisms** | **STRIDE Threats Mitigated** | **Reliability** | **Safety** | **Maintainability** | **Availability** | **Integrity** | **Confidentiality** | **Authenticity** | **Authorization** | **Non-repudiation** | **Freshness** | **Privacy** |
| Access control | T,I,D,E | N | + | N | - / + | + | + | N | ++ | N | + | + |
| Authentication control | S,R,E | + | - | N | + | N | + | ++ | + | + | + | + |
| Device authentication | S,T,R,E | + | + | N | + | ++ | N | ++ | + | + | + | N |
| Firewalls | T,I,D,E | N | + | + | + | ++ | ++ | + | + | + | + | + |
| Virtual networks | T,I,D | N | + | + | ++ | + | + | N | N | N | N | + |
| Encryption | S,T,I,E | + | + | N | - | ++ | ++ | ++ | + | + | + | ++ |
| Virtual Private Networks | S,T,I | + | + | N | N | ++ | ++ | ++ | + | + | + | ++ |
| Log auditing | R | + | + | ++ | + | + | + | N | + | ++ | + | + |
| Intrusion detection systems | S,T,R,I,D,E | + | + | N | + | + | + | + | + | + | + | + |
| Virus/malicious code detection systems | T | + | + | N | + | ++ | + | + | + | N | N | + |
| Vulnerability scanning | S,T,R,I,D,E | + | + | + | + | + | + | + | + | + | + | + |
| HCM and ASM tools | S,T,R,I,D,E | + | + | ++ | + | + | + | + | + | + | + | + |
| Operating systems | S,T,R,I,D,E | + | + | + | + | + | + | + | + | + | + | + |
| Web technologies | T,I | N | N | + | N | N | + | + | + | N | N | + |
| Physical security controls | S,T,R,I,E | N | + | N | N | + | + | + | + | + | N | + |
| Signatures | S,T,R | + | + | N | N | ++ | N | ++ | N | ++ | + | N |
| Partitioning and separation | T,I,E | + | + | + | + | + | + | N | + | N | N | + |

# Take away

Yesterday

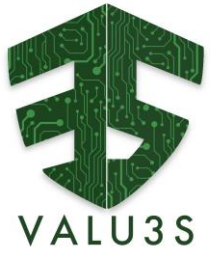
Safety and security analysis of computer systems *should* be done by a mixed group of safety and security experts.

Today

Analyses of the interplay between safety and security attributes is a *mindset* that should be integrated into the different phases of a system's development lifecycle.

# Acknowledgement


- Research projects and funding agencies







HoliSec

# Behrooz Sangchoolie

Analyses of the interplay between safety and security attributes in connected computer systems

behrooz.sangchoolie@ri.se

RI.SE