ASAF
28.3.2025

# Cybersecurity and functional safety comparison of risks

## COMMA-project results

**Timo Malm**

28/03/2025

Contents

**Published:**

# Comparison of cybersecurity and functional safety risk assessments

Link

RESEARCH REPORT VTT-R-00499-24


**Comparison of cybersecurity and functional safety risk assessments**

Authors: Timo Malm, Josepha Berger, Risto Tiusanen, Antti Ranta, Jari Seppälä, Bilhanan Silverajan, and Hanning Zhao

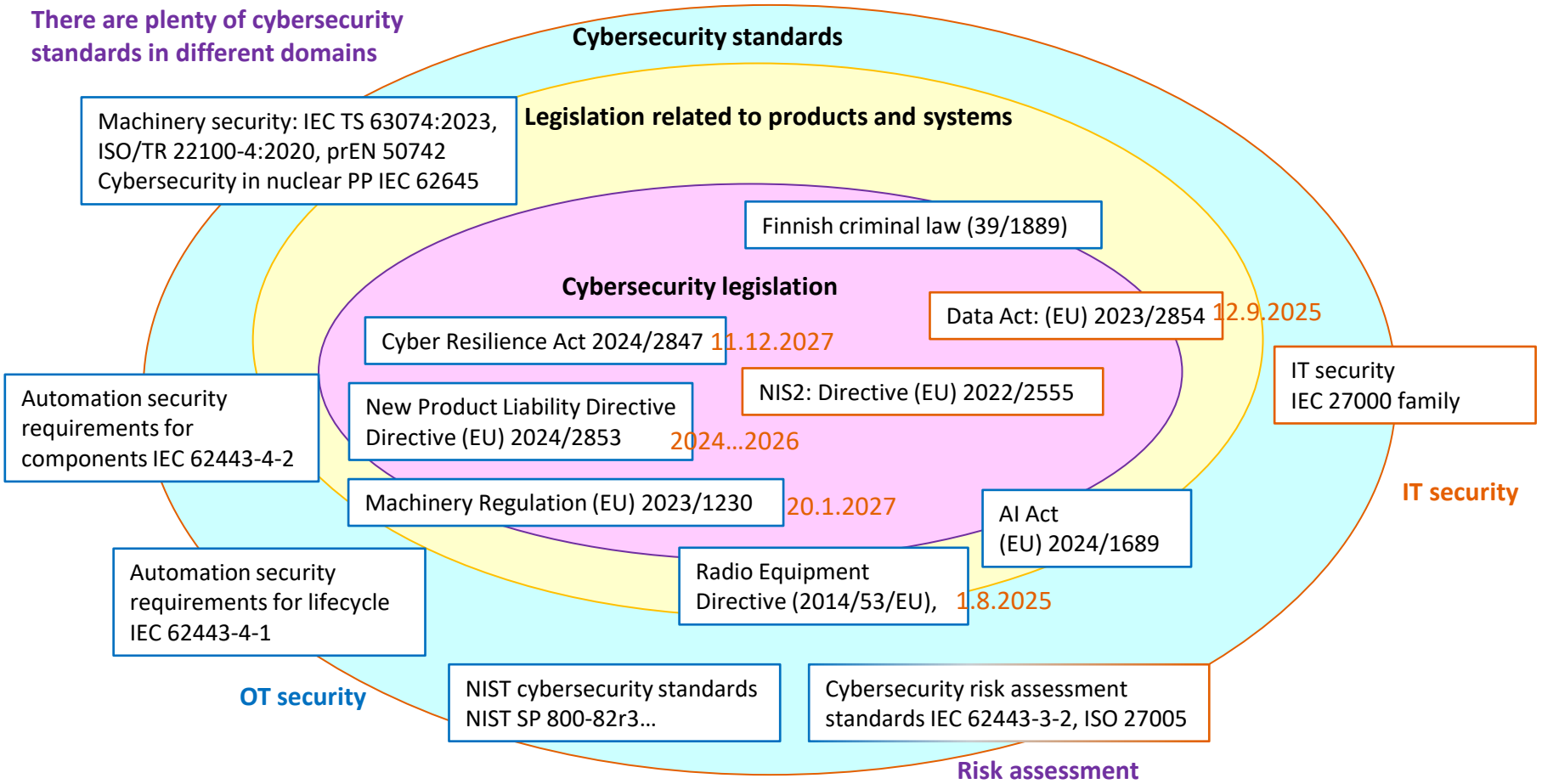
Confidentiality: Public

Version: 16.9.2024



"VTT-R-00499-24. Comparison of cybersecurity and functional safety risk assessments" : https://cris.vtt.fi/en/publications/comparison-of-cybersecurity-and-functional-safety-risk-assessment

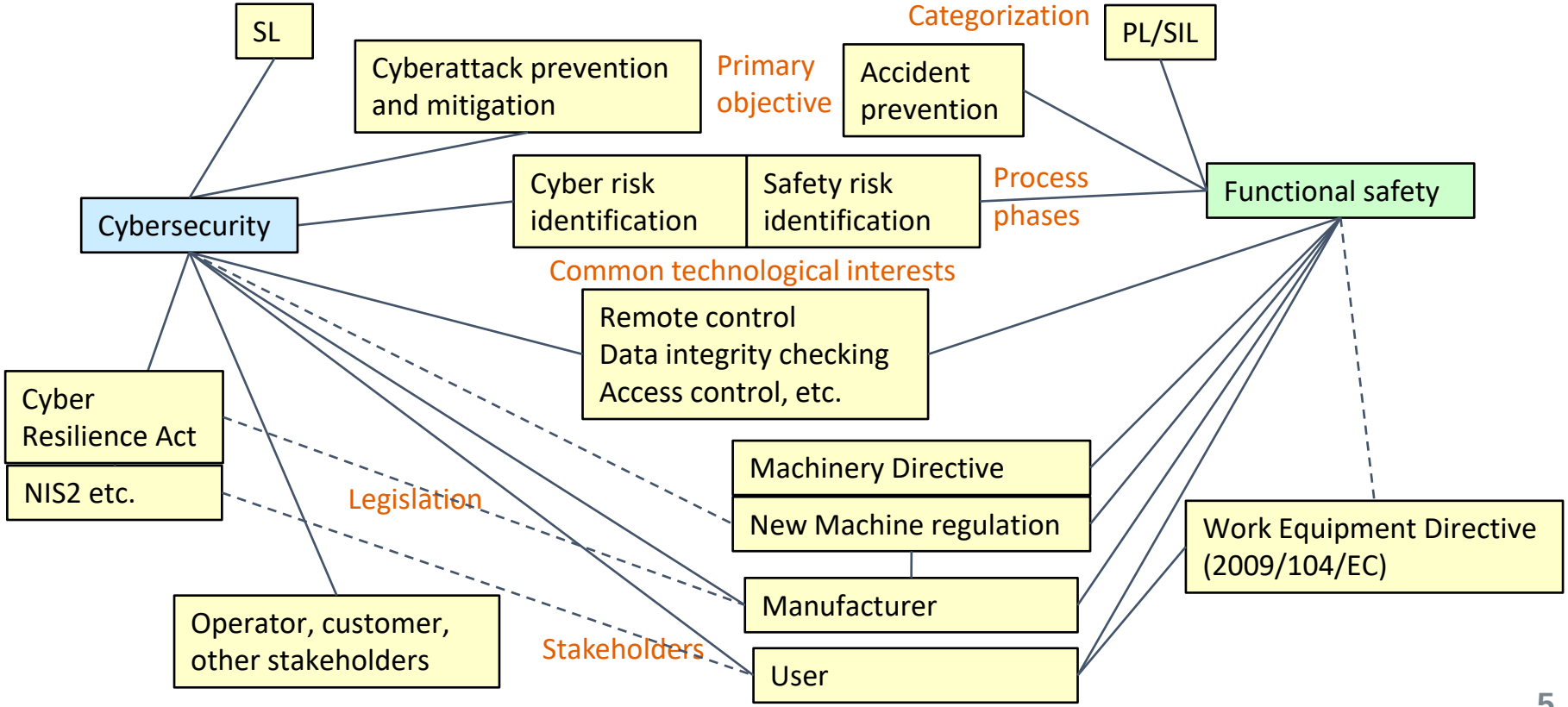
# Cybersecurity legislation – examples – sources of vulnerabilities



# Some main differences between functional safety and cybersecurity

| Topics | Safety viewpoint | Security viewpoint |
|---|---|---|
| Primary objectives | Injury/accident prevention, health Safety integrity is related to the probability of specified performance. | Negative impacts like, service problems, confidential information leak, integrity, preventing or minimizing cyberattack effects. |
| Victims, stake holders, | User (direct effect), bystanders | Asset owner, user, service provider, customers, etc. |
| Important attributes | Safety integrity (safety functions operate as planned), Availability (safety function available as planned) | OT systems: Availability, Integrity, Confidentiality<br><br>IT systems: Confidentiality, Integrity, Availability |

# Mindmap of cybersecurity and functional safety and examples of their relation to specific subjects

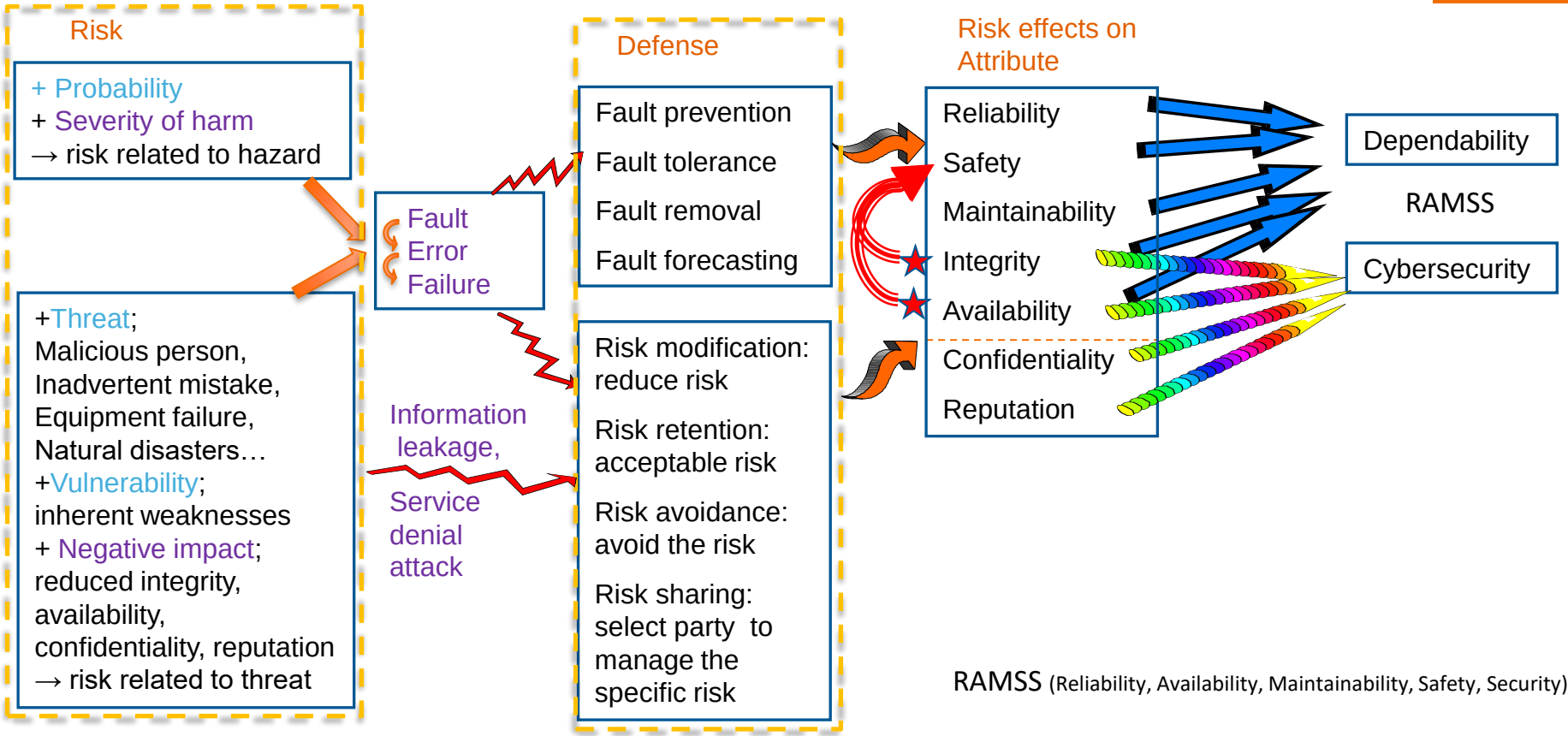


# Risk and risk reduction process parameters in safety and cybersecurity

Risk

| Safety | | Cybersecurity | |
|---|---|---|---|
| Severity of harm that can result from the considered hazard | Probability of occurence of that harm<br>Exposure of persons to the hazard the occurence of hazardous event the possibility to avoid or limit the harm | Possible negative impact that can result from the considered threat | Likelihood of that negative impact in relation to existing vulnerabilities that can be exploited by a threat |
| Hazard | Hazard identification | Threat | Circumstance or event effects |
| Severity | Criticality estimation | Vulnerability | Weakness that can be exploited by threat |
| Probability | | Impact | |
| Limits, properties | Risk reduction related to use | Likelihood | |
| Protective measures → Residual risk | | Assets, controls | Items that have an effect on cybersecurity |
| | | Countermeasures → Residual risk | |

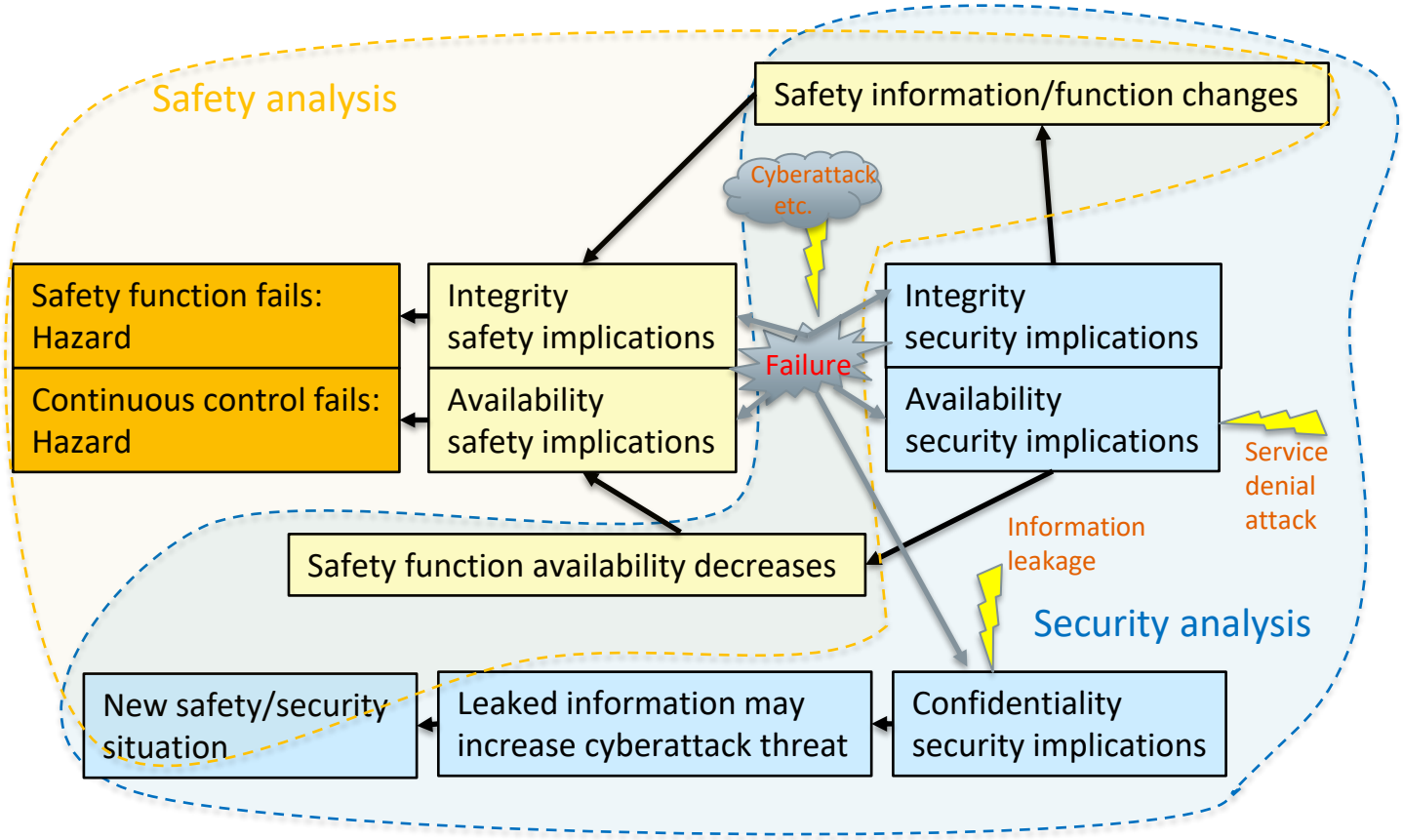
# Dependability and security taxonomy in programmable control systems



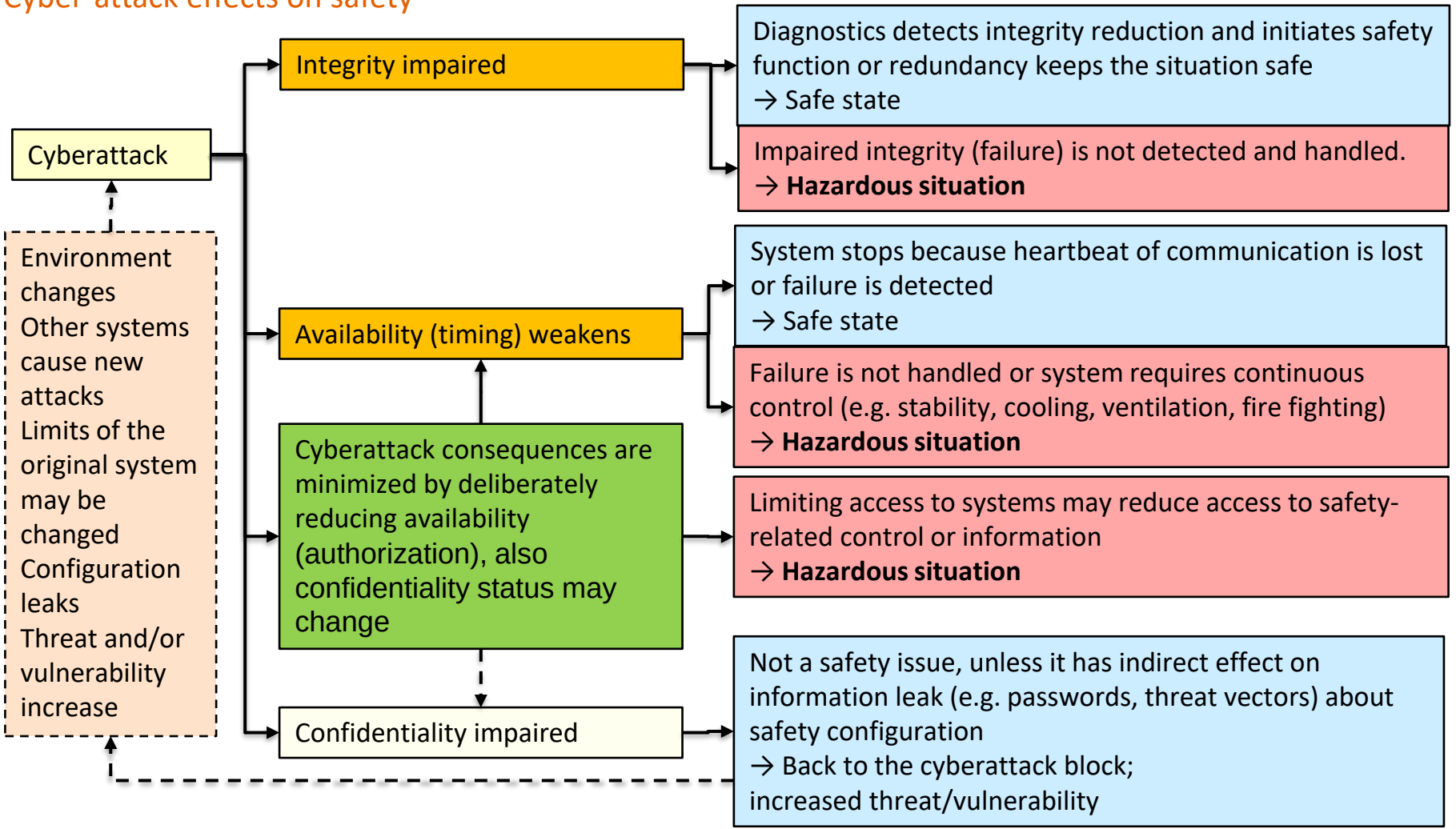

RAMSS (Reliability, Availability, Maintainability, Safety, Security)


Ref. Algirdas Avizienis, Fellow, IEEE, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing
ISO/TR 22100-4 Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects
IEC 27005:2018. Information technology. Security techniques. Information security risk management

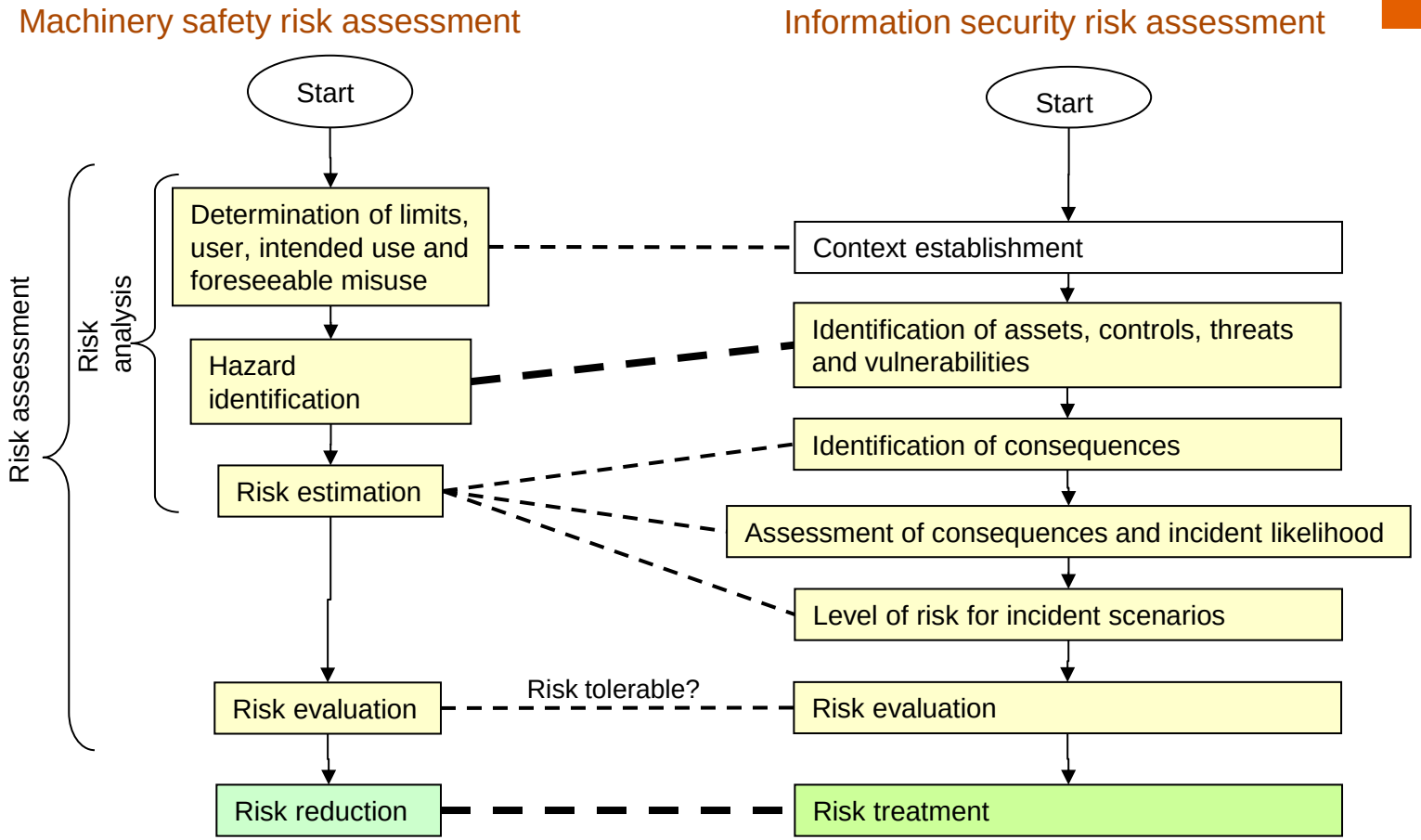
# Safety/security properties and risk analysis



# Cyber-attack effects on safety

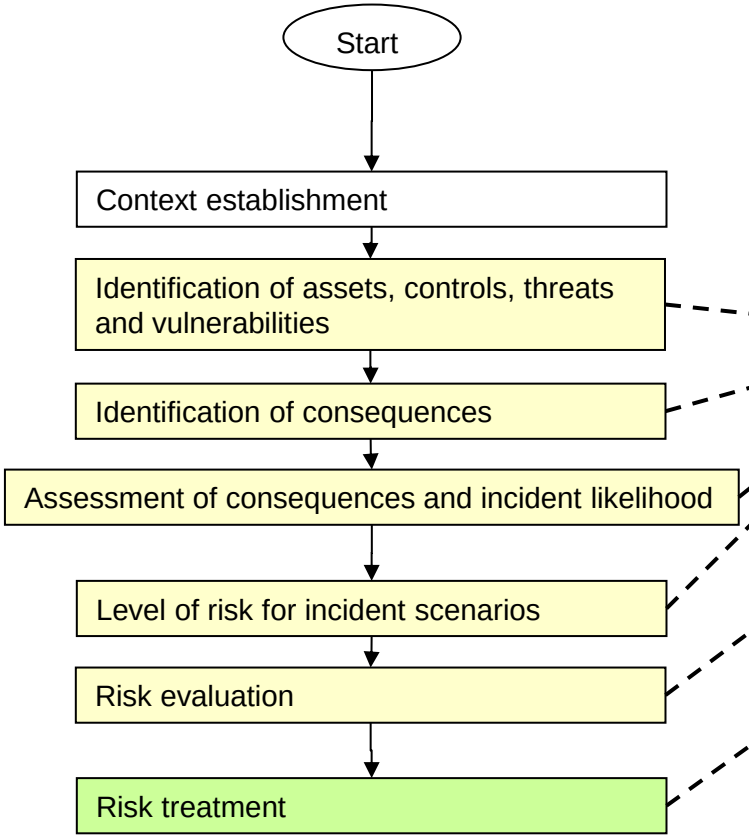


# Risk assessment (machinery) safety/security



# Risk assessment security

## Information security risk assessment




Ref. IEC 27005:2018

## Automation security risk assessment

ZCR 1: Identify the system under control

2. Initial cybersecurity risk assessment, identify worst case risks
3. Partitioning to zones and conduits,
Separate safety related assets,
Separate temporarily connected, external and wireless devices/networks
4. Compare risk to tolerable risk

5. Perform a detailed cyber security risk assessment
Identify threats, vulnerabilities,
Determine consequences and impacts
Determine unmitigated likelihood
Determine unmitigated cybersecurity risk
Determine SL-T

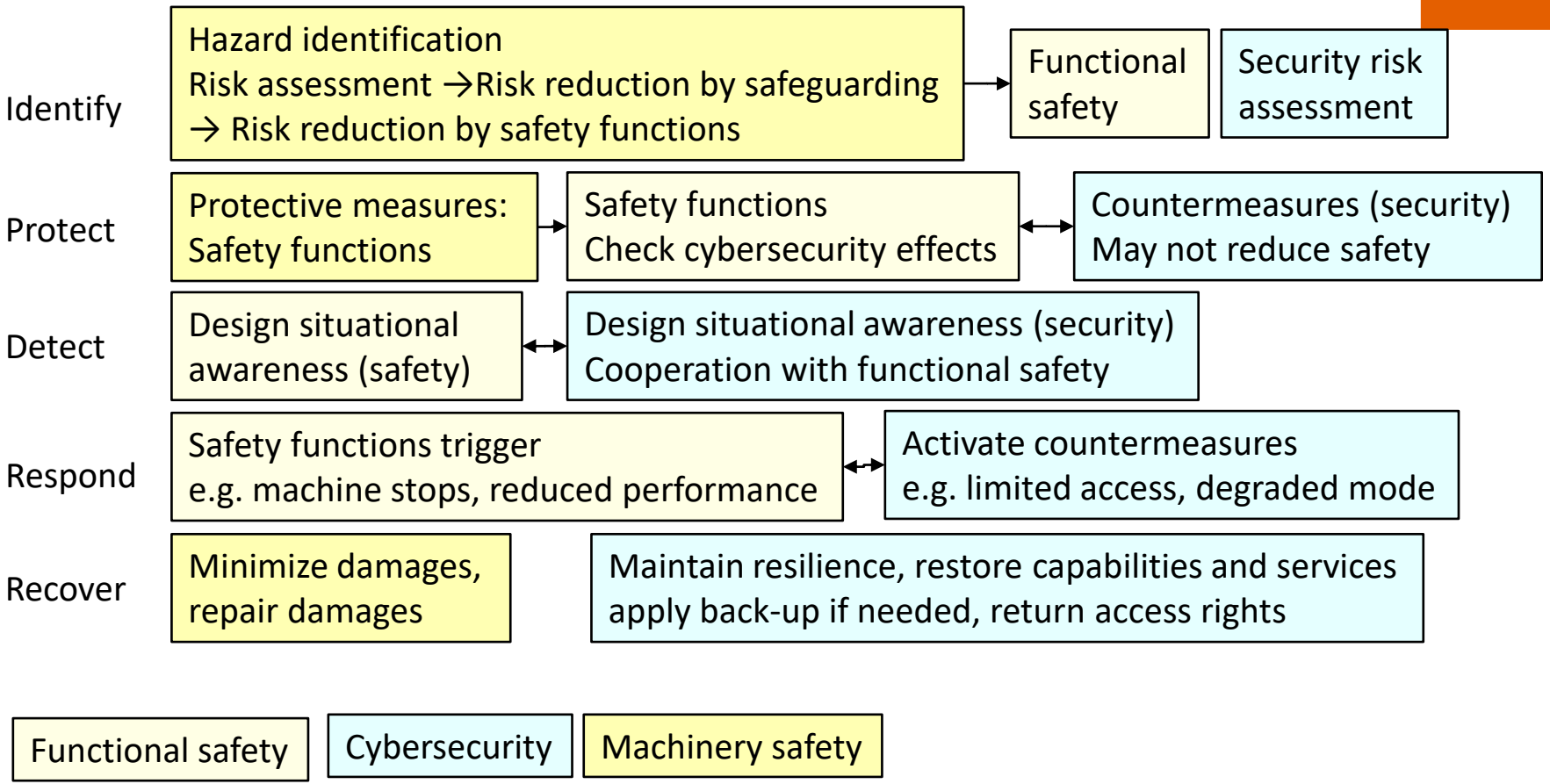
Compare unmitigated risk with tolerable risk

Identify and evaluate existing countermeasures
Reevaluate likelihood and impact, determine residual risk
Compare residual risk with tolerable risk
Identify additional cyber security countermeasures

6 Overall Cybersecurity documentation
7 Asset owner approval

IEC 62443-3-2:2020 Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design

# Security/safety steps to improve system with examples




ISO/TR 22100-4:2020. Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects.

# Several reasons, why safety and security analysis should be separate

- Objective is different: hazard/accident – negative impact
- Different requirements, categories (SL, SIL/PL) risks, objectives
- May be different: stakeholders, experts, liability, analysis intervals (cybersecurity analysis more often), system to be analysed, defence methods
- Separate or unified analysis:
  In bottom-up approach laborious due to many initial items.
  In top-down approach the no essential difference.

- However,

- Hazard/Threat/Vulnerability identification and risk reduction phase need cooperation.
- Cooperation in management and risk reduction methods

# Conclusions

- Select risk assessment method according to the needs
- In hazard/threat/vulnerability identification phase apply as many methods as needed, apply checklists.
- Check that risk reduction methods do not cause cybersecurity or safety problems.

# Thank you for your attention!

# Questions?



**Timo Malm**
Senior Scientist, MSc. (Tech)
System Safety

Tel. +358 20 722 3224
Email: timo.malm@vtt.fi

VTT Technical Research Centre of Finland Ltd
Visiokatu 4, Tampere
P.O. Box 1300
FI-33101 Tampere, Finland

www.vttresearch.com