Continental Engineering Services

Leveraging SOTIF Activities for Enhanced Cybersecurity

Stefan Wild | 29-May-2025

About Me @ Continental Engineering Services

Stefan Wild
Lead Engineer Cybersecurity & Privacy

Mail: stefan.wild@conti-engineering.com

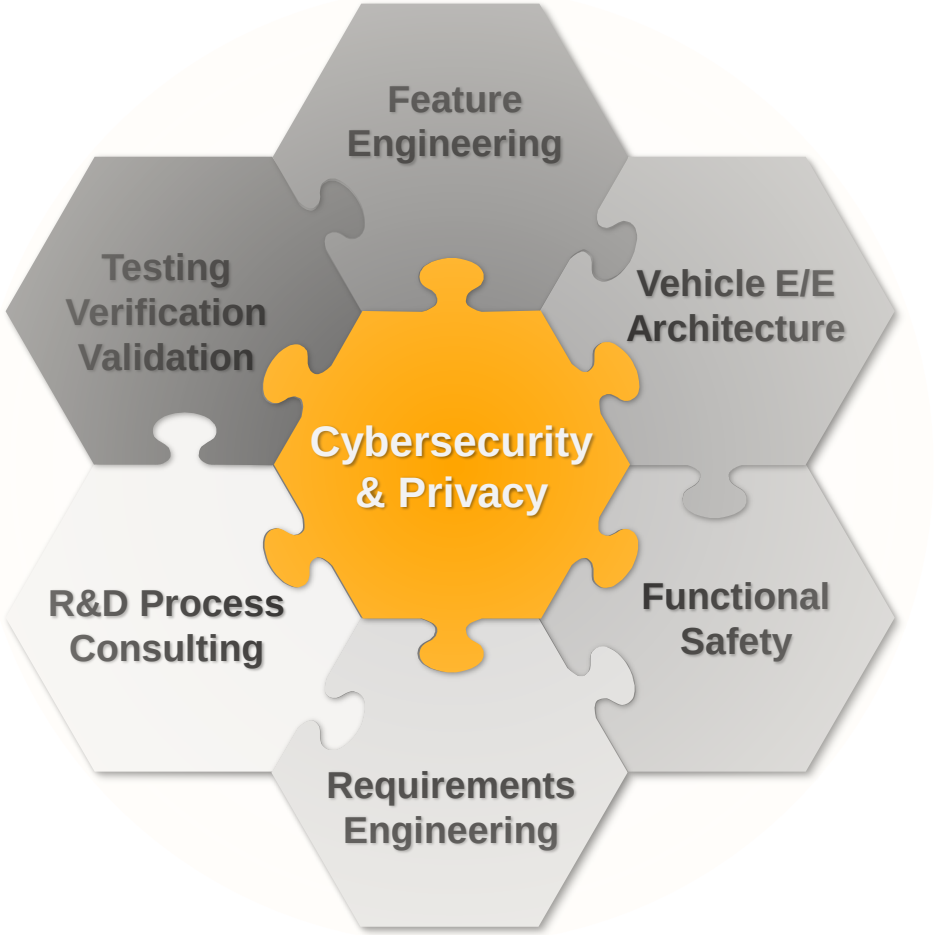
2022 Lead Engineer at Continental Engineering Services

- Process development for Automotive CSMS
- Cybersecurity assessments
- Cybersecurity risk management
- Acquisition and consulting

2016 Functional Owner Security

2016 PhD in Computer Science (Web Engineering, Security)

2008 Software Developer



CES Systems Engineering

Safety of the intended functionality (SOTIF)

Continental Engineering Services

- Diverse environmental conditions
- Lack of correct environment perception
- Lack of robustness of functions
- Unexpected behavior

Motivation

Considering ISO 21448 from a cybersecurity perspective

1 Cybersecurity

(Safety) of the intended functionality

2 cybersecurity

1 Cybersecurity of the intended functionality

2 Cybersecurity of the intended cybersecurity functionality

Cybersecurity threats are **not** in scope of ISO 21448:2022

Why relevant (in general)?

Continental Engineering Services

CrowdStrike Falcon Sensor Issue (2024)

Intended Functionality Detect and prevent cyber threats at the OS kernel level.
Shortcoming Faulty update caused memory error due to unchecked array length.
Impact Crashed and/or bricked ~8.5 million Windows systems, disrupting global infrastructure.

Heartbleed (2014)

Intended Functionality Secure communication via TLS/SSL encryption.
Shortcoming Flaw in heartbeat extension of OpenSSL allowed attackers to read memory from servers.
Impact Exposed sensitive data like private keys from major websites.

Colonial Pipeline Ransomware Attack (2021)

Intended Functionality IT/OT segmentation and access control.
Shortcoming Ransomware in IT systems led to a precautionary shutdown of OT systems.
Impact Fuel shortages across the US East Coast.

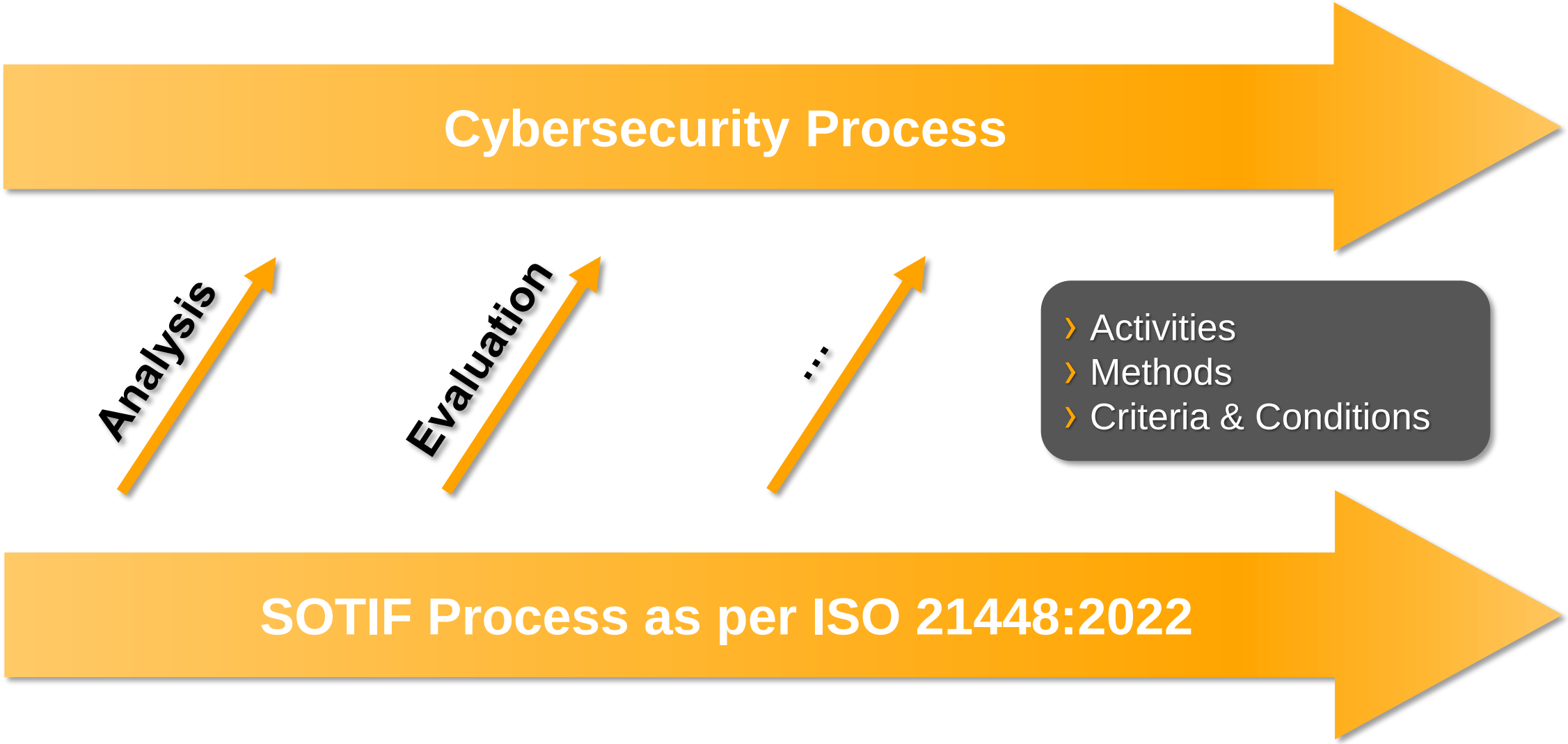
Okta Breach (2022)

Intended Functionality Identity and access management (IAM).
Shortcoming Compromise of 3rd party support provider led to unauthorized access to Okta's internal systems.
Impact Potential exposure of customer data and trust loss.

SolarWinds Orion Supply Chain Attack (2020)

Intended Functionality Network monitoring and security management.
Shortcoming Attackers inserted backdoor into SW update, which was distributed to thousands of customers.
Impact Breach of US gov. agencies and Fortune 500 companies.

Approach
Considering ISO 21448 from a cybersecurity perspective



Disclaimer

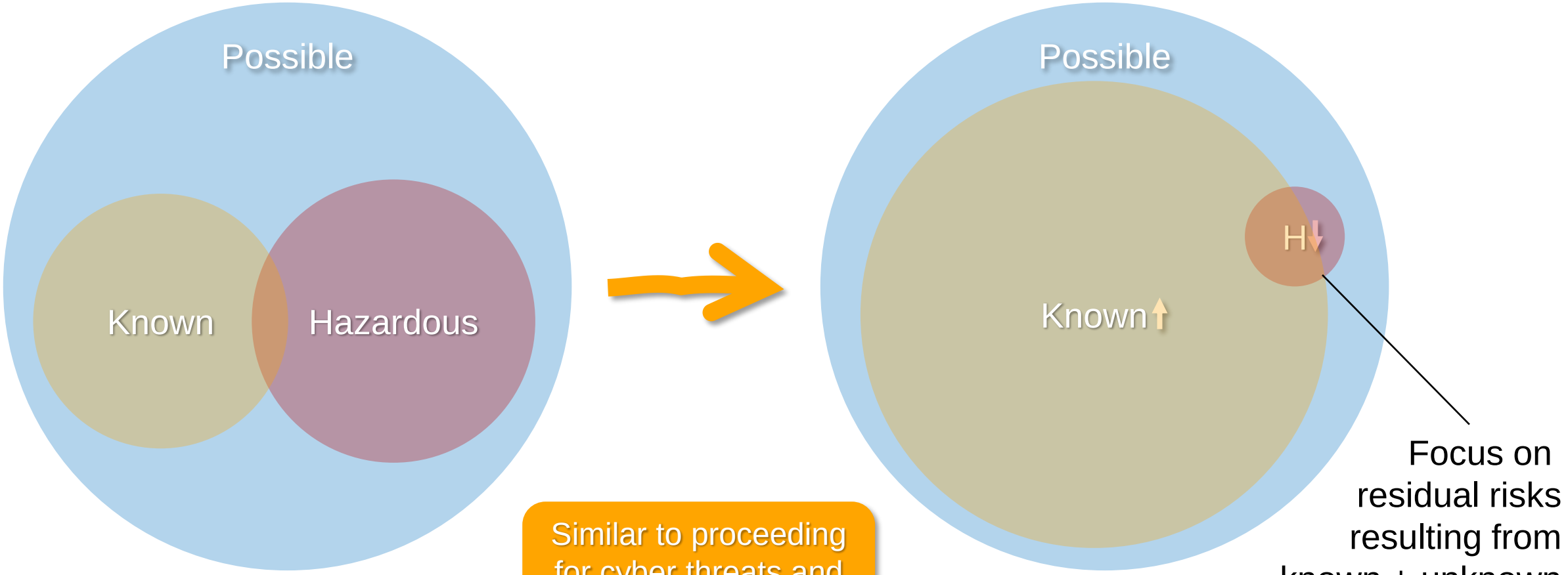
I am not an expert of functional safety or of SOTIF.

The presentation is about a consideration of SOTIF process elements from the perspective of cybersecurity.

A fundamental understanding of cybersecurity, functional safety and SOTIF on the basis of the corresponding ISO standards is expected.

SOTIF principles and activities

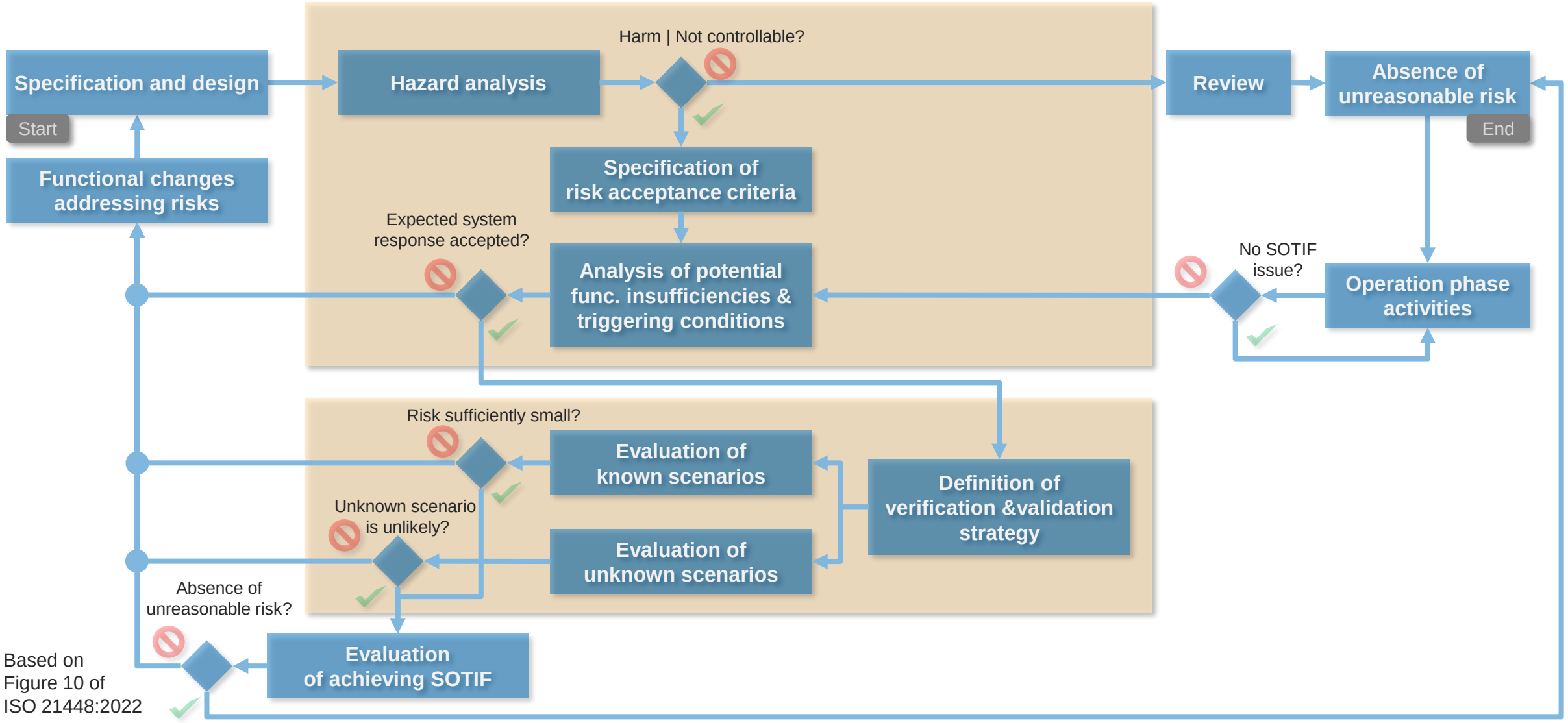
SOTIF principles and activities
Scenarios evolution



Similar to proceeding for cyber threats and resulting cyber risks

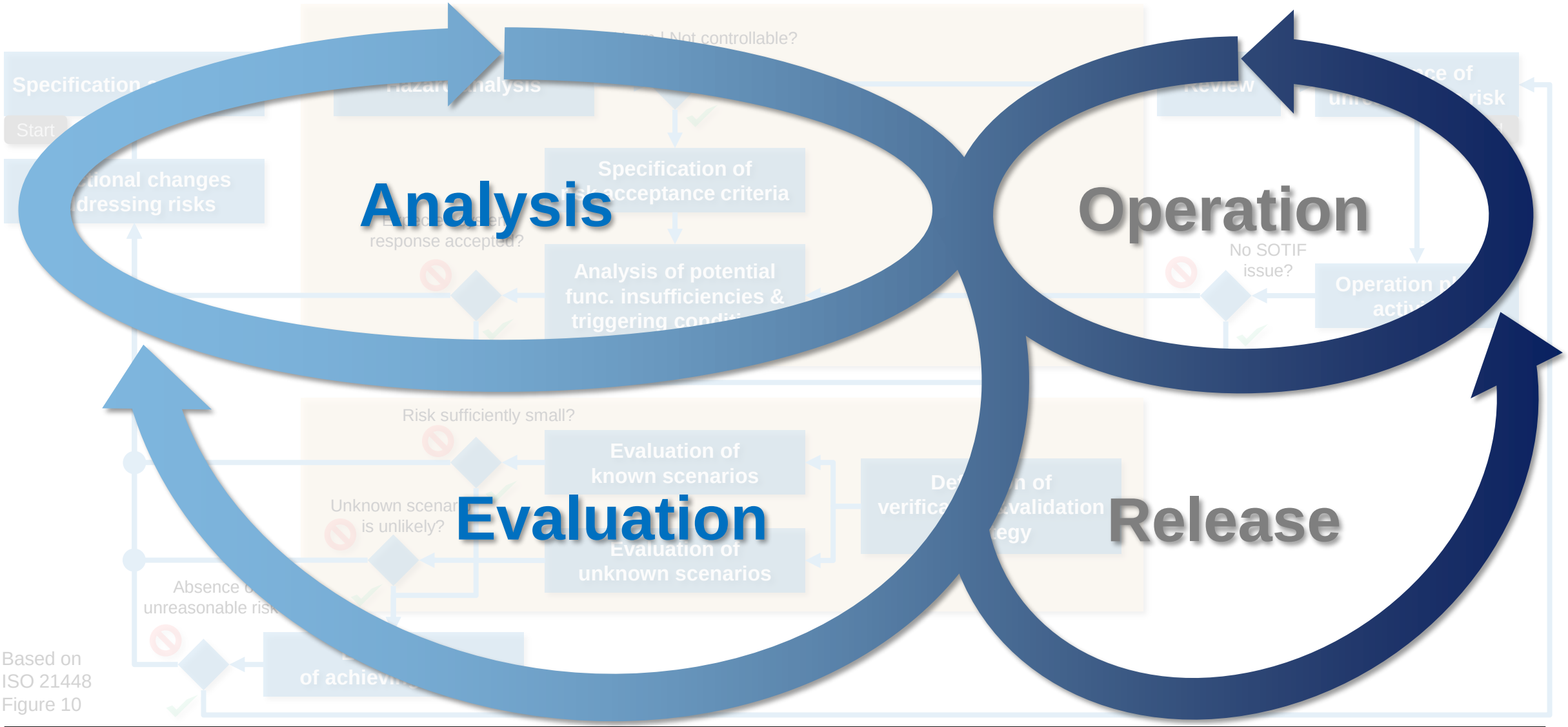
Based on Figure 7 of ISO 21448:2022

SOTIF activity model according to ISO 21448

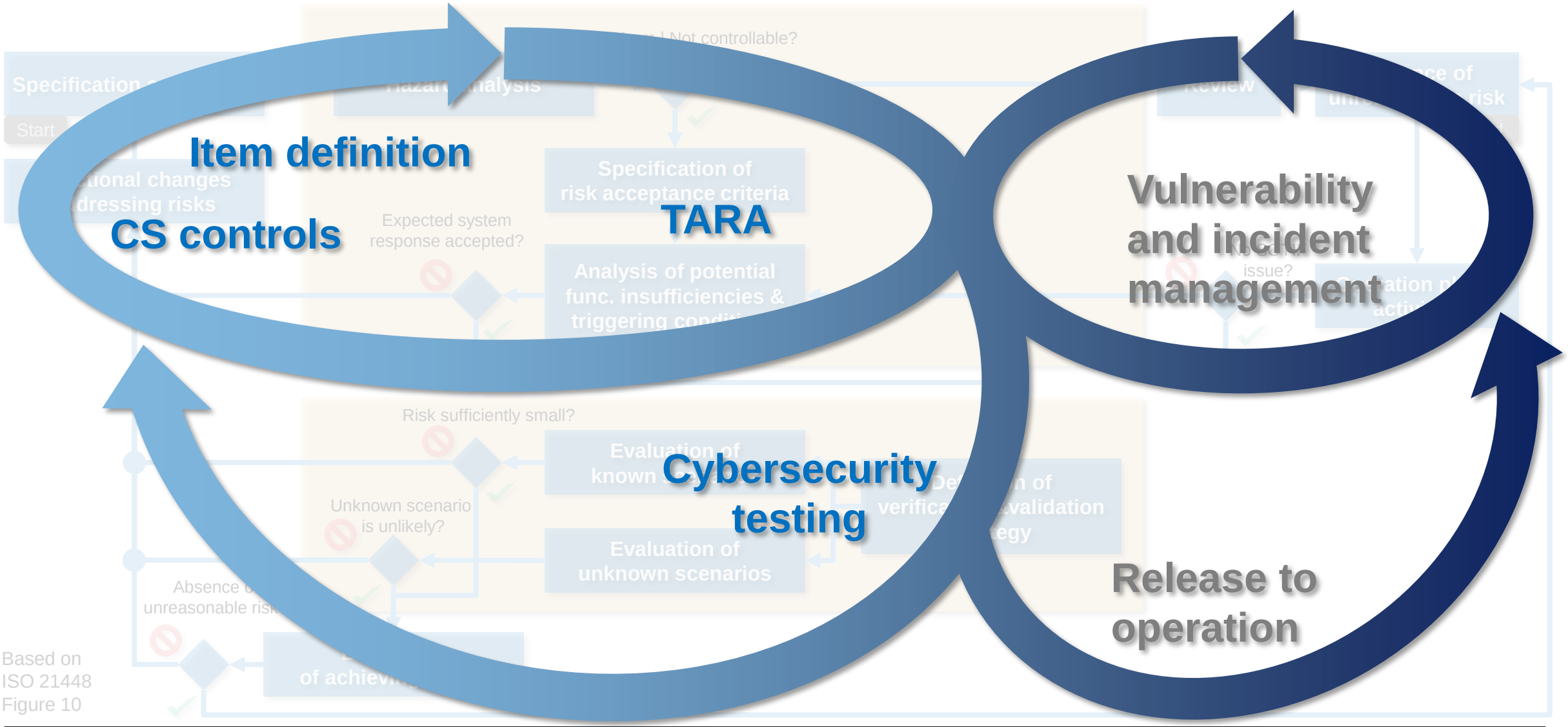


Based on Figure 10 of ISO 21448:2022

SOTIF activity model: Abstracted iterations & increments



An *idealized* cybersecurity perspective on SOTIF activity model



Analysis

From the perspective of cybersecurity

Analysis

Item definition enriched with details on intended functionality

Continental Engineering Services

- Description of intended functionality
- Dependencies, interactions, interfaces of the intended functionality
- Potential performance insufficiencies, identified triggering conditions and countermeasures
- System design and architecture related to the intended functionality
- Reasonably foreseeable misuse (direct and indirect)
- Data collection and monitoring
- Warning and degradation concept
- Mechanisms to support risk mitigation during operation
- Performance targets

Largely applicable to cybersecurity

Based on Section 5.2 of ISO 21448:2022

Analysis
Identification

Continental Engineering Services

Subject

› Hazards arising from intended functionality

› Risks arising from hazardous behavior

“Identification is primarily based on knowledge about the **function** and its **possible deviations** resulting from **functional insufficiencies**.”

Considerations for **residual risk acceptance**

✓ Applicable governmental/industry regulations

✓ Novelty of function in the market

✓ Pre-existing criteria from similar functions

✓ Risk perception by stakeholders

Data → **Function** → **Data**

- Payloads
- Signals
- Requests
- Arguments

…

- Vehicle functions
- Vehicle system functions
- System product functions

…

- Payloads
- Signals
- Responses
- States

…

Cybersecurity analysis of triggering malfunctions

Based on Section 6.1, 6.3 and 6.4 of ISO 21448:2022

Analysis
Potential functional insufficiencies and triggering conditions

Subject

- Known and determined potential insufficiencies
  - Insufficiencies in specification
  - Performance insufficiencies
- Identified environment conditions
- Identified reasonably foreseeable misuse

Largely applicable to cybersecurity

Scope of analysis methods

- Requirements
- Operational design domain
- Use cases and scenarios
- Boundary values
- Functional dependencies
- Triggering conditions
- System design & architecture
- Possible env. changes over operational lifetime
- Technology limitations / algorithms
- External & internal interfaces
- Assumptions

Measures needed if

- Residual risks not matching acceptance criteria
- Known scenarios leading to unreasonable risks

Avoidance measures	Mitigation measures
Risk avoidance	Risk reduction

- ✓ No adverse effects on other system elements
- ✓ No interactions with other hazardous scenarios

Based on Section 7.3 and 7.4 of ISO 21448:2022

Evaluation

Evaluation
Verification and validation strategy

Subject

- Evaluation of potentially hazardous scenarios
- **Sufficient coverage** of relevant scenarios
- **Validation targets** to meet acceptance criteria of residual risks
- **Evidences** needed and how to obtain
- **Justifications** for selected V&V methods

Scope of analysis methods to derive V&V activities

- Requirements
- Operational use, corner and edge cases
- Collected test cases and scenarios
- Error guessing based on knowledge or experience
- Triggering conditions
- System design & architecture
- External & internal interfaces
- Functional dependencies
- Boundary values
- Known limitations

Largely applicable to cybersecurity

Based on Section 9.3 of ISO 21448:2022

Evaluation
Known scenarios

Subject

- Evaluate identified potentially hazardous scenarios if hazardous or not
- Cover known scenarios sufficiently
- Demonstrate that validation targets are met
- Check that system behaves as specified and if potentially hazardous behavior is acceptable

Methods

- Verification methods for SPA and integrated systems

Goal setting

- Probability of known scenarios causing hazardous behavior matches validation targets
- Residual risk from known hazardous scenarios is not unreasonable

Similar to white box testing for cybersecurity

Based on Chapter 10 of ISO 21448:2022

Evaluation
Unknown scenarios

Subject

- Demonstrate that “residual risk from *unknown* hazardous scenarios meets the acceptance criteria with sufficient confidence”
  - Like encountered unknown scenarios less than specified threshold

Verification and validation methods

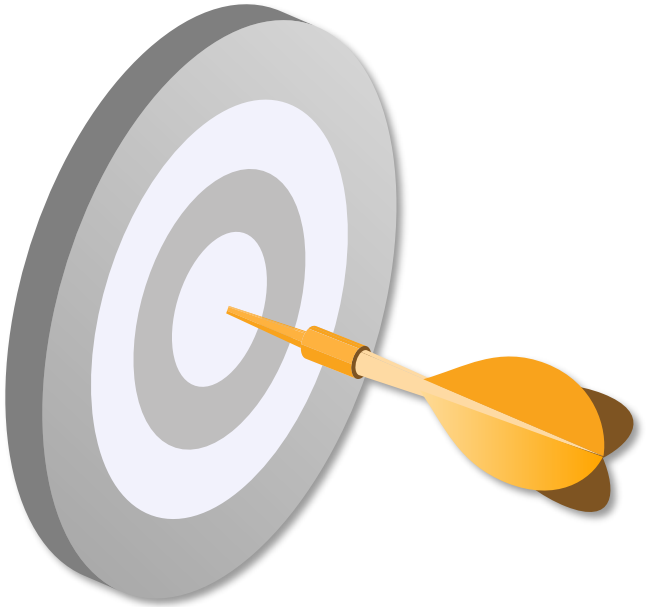
- Robustness validation (like **noise injection testing**)
- **Randomized test cases** / input tests
- Simulation of relevant parameters
- Test of potential misuses with **random usage**
- Simulation based on **random sequence of scenarios**
- Scenario **exploration** in real world

Similar to black/gray box and fuzz testing for cybersecurity

Based on Chapter 11 of ISO 21448:2022

Conclusion

Conclusion



- ✓ Surprising level of overlap to cybersecurity and even beyond
- ✓ Don’t underestimate the evolutionary steps done elsewhere
- ✓ Get involved with other engineering discipline
- ✓ Read and discuss *related* standards
- ✓ Less silo thinking
- ✓ Utilize the good parts
- ✓ Benefit from interdisciplinary experiences and synergies **@CES**

Questions and Answers

Stefan Wild
Lead Engineer Cybersecurity & Privacy
Systems Engineering
Continental Engineering Services GmbH

Mail: stefan.wild@conti-engineering.com

Thank you