AGRARSENSE

Adapting ISO 21448 for Mobile Machinery
A Forestry Automation Case Study

Marvin Damschen, Kristian Flink, Aria Mirzai - RISE

The project is supported by the Chips Joint Undertaking and its members, including the top-up funding by Sweden, Czechia, Finland, Ireland, Italy, Latvia, Netherlands, Norway, Poland, Spain.

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

PURPOSE

- Structure a **safety case** for semi-autonomous forestry machinery, **focused on a human detection system**

- Demonstrate how ISO 21448 (SOTIF[1]) can be adapted to the conditions and regulations of off-road forestry

- SOTIF aims to **show that residual risk stays below acceptable levels, despite perception errors, sensor degradation, or edge-case environments**

[1] Safety of the Intended Functionality
[2] Verification and Validation

OUTLINE

REGULATORY CONTEXT AND CHALLENGES

ROLE OF THE SAFETY SYSTEM IN AUTONOMY

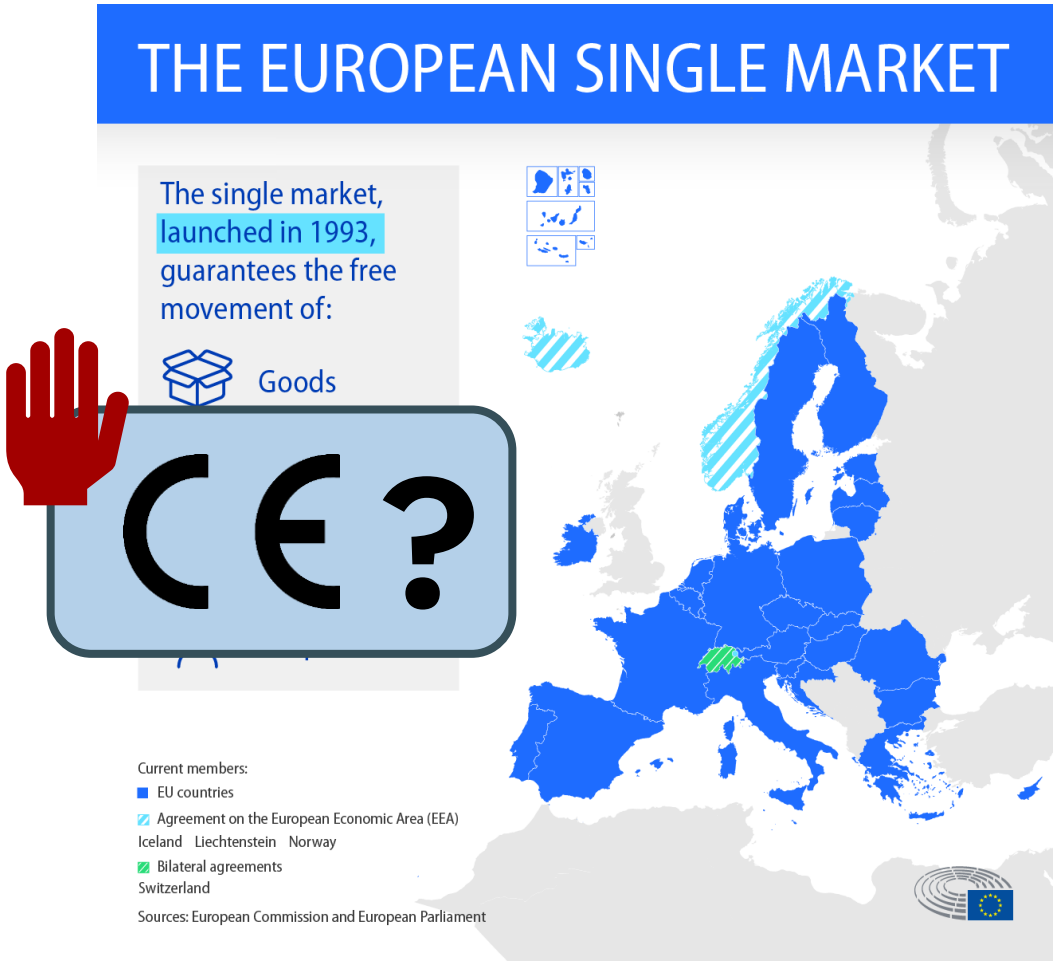
SOTIF PROCESS FOR FOREST MACHINERY

REAL WORLD EXPERIMENTS AND COLLABORATIVE SYSTEM SAFETY


AGRARSENSE
REGULATORY CONTEXT AND CHALLENGES

REGULATORY CONTEXT

- Autonomous forestry machinery must satisfy **Regulation (EU) 2023/1230**
- The regulation anticipates a greater role for software and sensors in decision-making
- Unlike how SOTIF complements ISO 26262[1] in automotive, **mobile machinery lacks harmonised EU standards for intended functionality**



[1] ISO 26262: Road vehicles – Functional safety

REGULATORY CHALLENGES

- Existing machinery standards (ISO 12100[1], ISO 13849[2]) offer limited guidance on probabilistic sensor performance, runtime monitoring, or on perception faults

  → **Conceived for deterministic mechanical and electrical failures**

- As reliance on CV[3], LiDAR[4], and AI grows, standards must evolve to include **probabilistic metrics, SOTIF-style edge case analysis, and runtime monitoring for early fault detection**

[1] ISO 12100: Risk assessment and risk reduction
[2] ISO 13849: Safety-related parts of control systems
[3] Computer Vision
[4] Light detection and ranging


AGRARSENSE
ROLE OF THE
SAFETY SYSTEM IN
AUTONOMY

AUTONOMOUS MOBILE MACHINERY

- Use case: Shuttle transports logs from a harvester along pre-mapped forest roads to drop-off point (loading/unloading handled by external machinery)

- Supervisory staff receive live telemetry and video—can trigger human override or safe state

- **Hazard = Humans can get run over**
  → Need a safety-critical system that can detect people

ENVIRONMENTAL CHALLENGES

- Complex and unpredictable environment: Variable surface quality, steep gradients, rapidly changing light conditions, heavy occlusion …

- **People may enter the machine's workspace unexpectedly**, linger in sensor blind spots or alter their movement signature

- **The safety system must detect people reliably across a broad ODD[1] and execute safe-state transitions under degraded perception**

[1] Operational Design Domain

SAFETY AROUND THE FORESTRY SHUTTLE

- **Hazard zone**: Shuttle's maximum stopping distance plus a safety margin

- Active/passive measures:

  - Geofenced route enforcement
  - Remote-supervision heartbeats
  - Audible & visible warning signals
  - **Safety system for detecting people**

- **Any safety trigger occurrence (e.g. an ODD violation such as heavy occlusion) engages the "safe state"**


AGRARSENSE
SOTIF PROCESS FOR
FOREST MACHINERY

SOTIF ADAPTATION CHALLENGES

- Transferring SOTIF from the well-regulated, data-rich context of road vehicles to off-road forestry machinery offers both alignment and challenge:

  + Increased reliance on CV[1], LiDAR, and ML-technologies whose failure modes and performance metrics echo those found in ADAS[2]

  - Forest environments differ in speed, terrain, lighting, and data availability, making automotive risk principles (ALARP[3], PRB[4]) harder to quantify

- **Big advantages: Slower speed (10km/h) + Can stop at any danger**

[1] Computer Vision
[2] Advanced Driver Assistance Systems
[3] As Low As Reasonably Practicable
[4] Positive Risk Balance

SPECIFICATION AND DESIGN (CLAUSE 5)

- Requires capturing the intended functionality in a detailed specification

- **Narrowed case study:**

  (safety) System comprises a front RGB-D[1] camera feeding point-cloud and intensity data into a CNN[2] based perception pipeline in a constrained ODD[3]

Source: traxxas.com/88086-84-trx-6-flatbed-hauler-winch

- Control authority strategy: **”Fail-stop”**
  → Contrasts with automotive SOTIF approaches

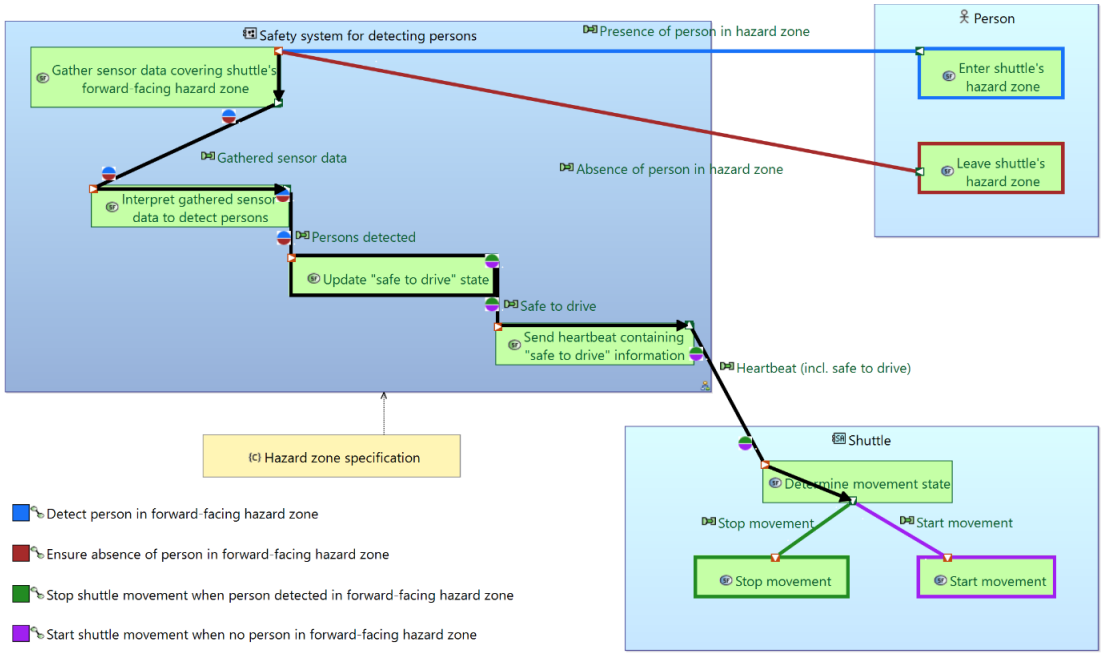
[1] Red Green Blue – Depth
[2] Convolutional Neural Network
[3] Operational Design Domain

SPECIFICATION AND DESIGN (CLAUSE 5)

- Design considerations must be documented and maintained as the SOTIF analysis evolves

- **Employed MBSE[1] (Capella)**, which structures the specification across four abstraction layers: Operational, System, Logical, Physical

- Although not a SOTIF requirement, MBSE enables traceability from high-level safety goals to low-level software and hardware components



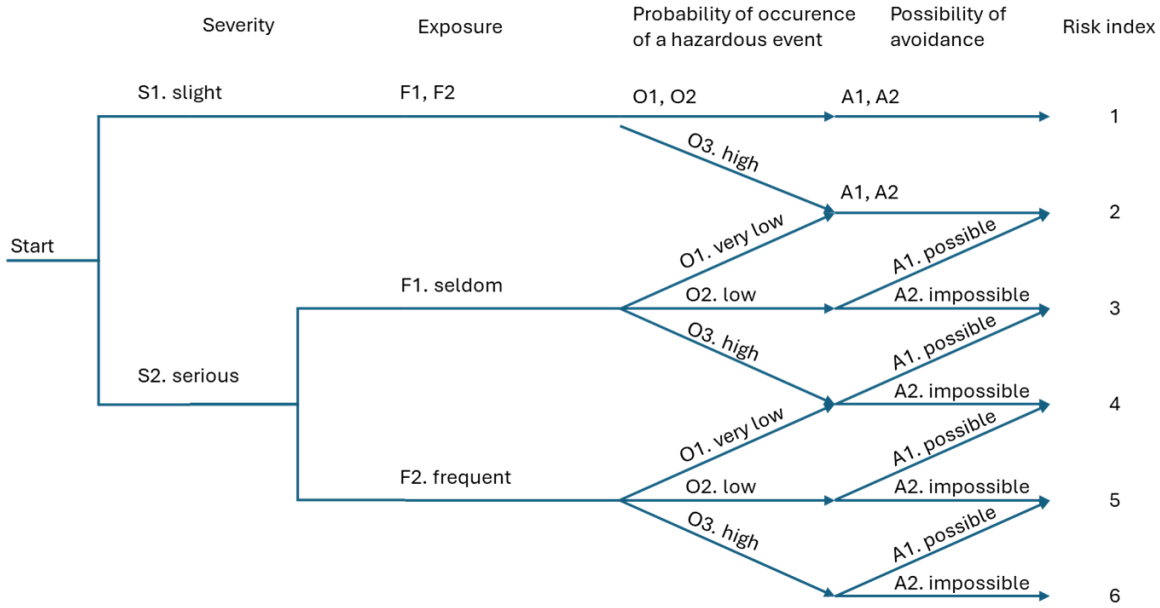
System Architecture

[1] Model-Based Systems Engineering

HAZARD ANALYSIS (CLAUSE 6)

- SOTIF suggests adopting ISO 26262-3 (HARA[1])

- However, **mobile machinery can instead leverage ISO 12100[2] and ISO/TR 14121-2[3]** to assess the risk-driving parameters:
  - Severity (S)
  - Frequency of exposure (F)
  - Occurrence (O)
  - Avoidance (A)



ISO/TR 14121's risk graph

[1] Hazard Analysis and Risk Assessment
[2] ISO 12100: Risk assessment and risk reduction
[3] ISO/TR 14121-2: Risk assessment

ACCEPTANCE CRITERIA (CLAUSE 6)

- For automotive, SOTIF suggests defining acceptance criteria by applying:
  - GAMAB - Guidelines for the Acceptability of Motorized Automobile Behaviour
  - PRB - Positive Risk Balance
  - ALARP - As Low As Reasonably Practicable
  - MEM - Manageable Exposure Metric

- **However, due to the scarcity of large-scale forestry accident statistics, other ways to define acceptance criteria are needed**

- One option is to use ISO 13849-1[1] performance levels for average probability of dangerous failure per hour …

[1] ISO 13849: Safety-related parts of control systems

ACCEPTANCE CRITERIA (CLAUSE 6)

- … together with UL 4600[1]-style **Safety Performance Indicators (SPI)** to support continuous safety monitoring and define acceptable hazard rates **(e.g. “undetected-person events per x km”)**

- **Each SPI serves as a validation target** for simulations, test-track trials, and field monitoring—providing evidence that the acceptance criteria are met

- Linking real-world data, SPI:s and safety arguments **enables continuous SOTIF validation throughout a system’s operational life**

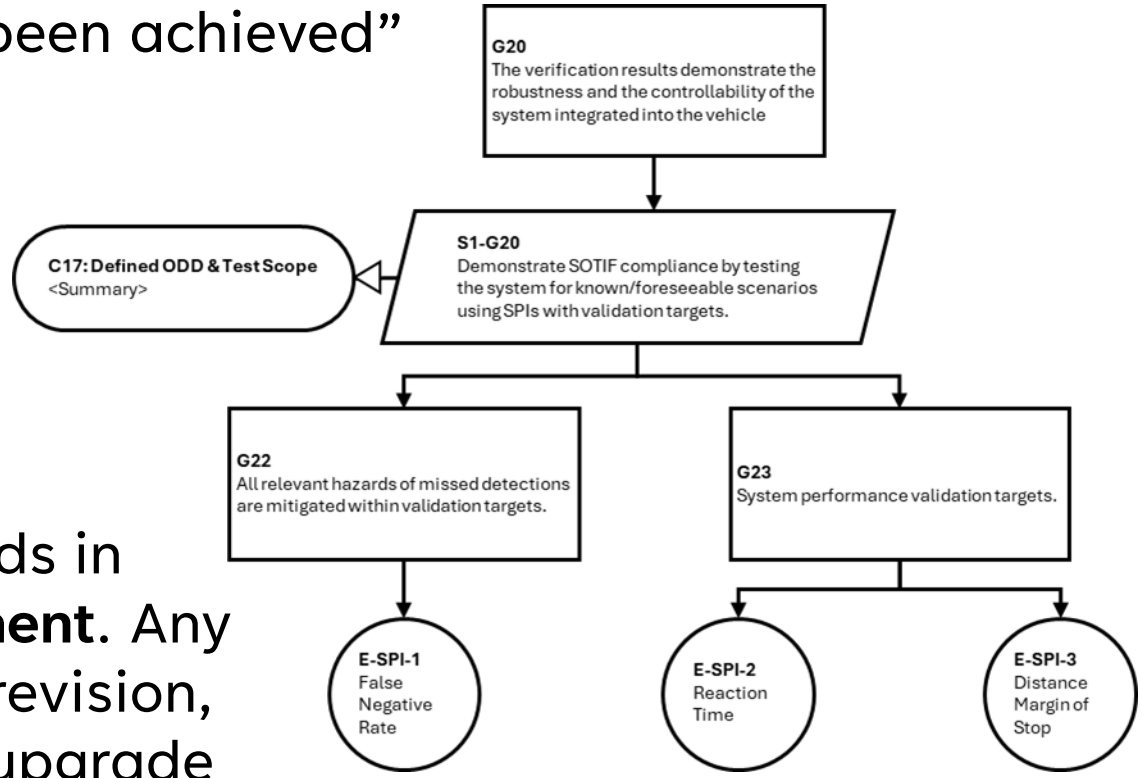
[1] UL 4600: Standard for Evaluation of Autonomous Products

SOTIF ARGUMENT USING GOAL STRUCTURING NOTATION (GSN)

- Top claim (G1): “The absence of unreasonable risk due to hazards associated with the intended functionality or its reasonably foreseeable misuse has been achieved”

- UL 4600[1]-style **SPI:s[2] supports residual risk arguments by feeding evidence into relevant safety goals**

- Linking SPI:s to acceptance thresholds in GSN creates a **“living” safety argument**. Any jeopardized claim triggers a design revision, ODD tightening, or countermeasure upgrade



[1] UL 4600: Standard for Evaluation of Autonomous Products
[2] Safety Performance Indicator


AGRARSENSE
REAL WORLD
EXPERIMENTS AND
COLLABORATIVE
SYSTEM SAFETY

MODEL-SCALE PROTOTYPING (ISO 21448, TABLE 10-G)

- Not intended to provide reliable performance figures, nor fulfil actual SOTIF compliance standards

- **Show how real-world experiments can be linked to a GSN[1] safety argument via SPI:s[2] (e.g. false negative rate, distance estimation error, reaction time delay)**

- Real-world tests show how easily risks emerge (sensor anomalies, occlusion effects, light failures) which are complex to mitigate in subsequent SOTIF cycles

[1] Goal Structuring Notation
[2] Safety Performance Indicator

COLLABORATIVE SUPERVISION

- **Can assume ground-only sensing will have shortcomings**: branches covering sensors, trees, slopes, boulders, etc.

- UAS[1] with RGB & thermal payload field tested as **on-demand aerial sensors**, to spot hidden personnel and obstacles

- This collaborative concept remains at the feasibility-investigation stage (putting safety-critical functionality on a drone is a project in itself)

[1] Unmanned Aerial System

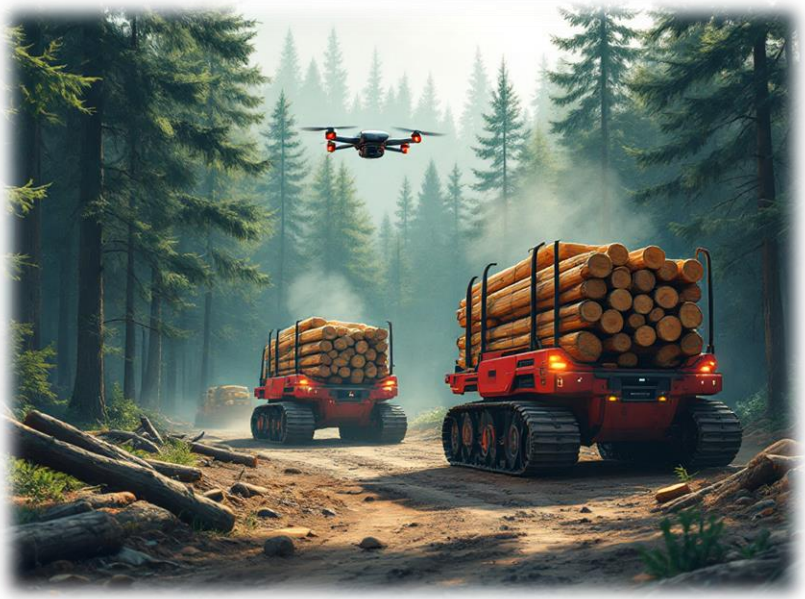

AGRARSENSE
CONCLUSIONS

CONCLUSIONS

- **THE BIG NEWS: Adopting SOTIF for machinery is pretty straightforward** (one big advantage over automotive: Can brake at any danger)

- **Violating SPIs linked to validation targets in the safety argument can trigger risk mitigating iterations—even after deployment**

- Unresolved: SOTIF **acceptance criteria like "performs as an exemplary human driver" require extensive data**—available in automotive, but lacking for machinery



Generated using FLUX1.1

QUESTIONS?

Aria Mirzai

aria.mirzai@ri.se

(company profile)