New requirements related to cybersecurity and AI

Safety of Machinery challenges

Jean-Christophe Blaise - INRS

Institut National de Recherche et de Sécurité

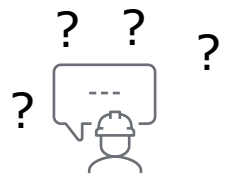
EUROSHNET

Summary

Machnirey Regulation

(EU) 2023/1230

Context: MR (EU) 2023/1230



Designers

Machinery Regulation 2023/1230

- Cybersecurity
- Artificial Intelligence

Cyber Resilience Act 2024/2847

NIS 2 Directive (EU) 2022/2555

The Cybersecurity Act 2019/881

RED Directive 2014/53/EU

AI Act 2024/1689

Guide to application EU Commission

Safety of machinery standards

UNM

guides

02

Cybersecurity in machinery

Security & Safety

Cybersecurity Requirements in annex III

1.1.9 Protection against corrruption (extract)

A hardware component transmitting signal or data, relevant for connection or access to software that is critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be designed so that it is adequately protected against accidental or ***intentional corruption****. The machinery or related product shall collect evidence of a legitimate or* ***illegitimate intervention*** *in that hardware component, when relevant for connection or access to software that is critical for the compliance of the machinery or related product*)

1.2.1 Safety and reliability of control systems in particular a) and f)

Control systems shall be designed and constructed in such a way that:

a) they can withstand, where appropriate to the circumstances and the risks, the intended operating stresses and intended and unintended external influences, including reasonably foreseeable malicious attempts from third parties leading to a hazardous situation.

Ressources

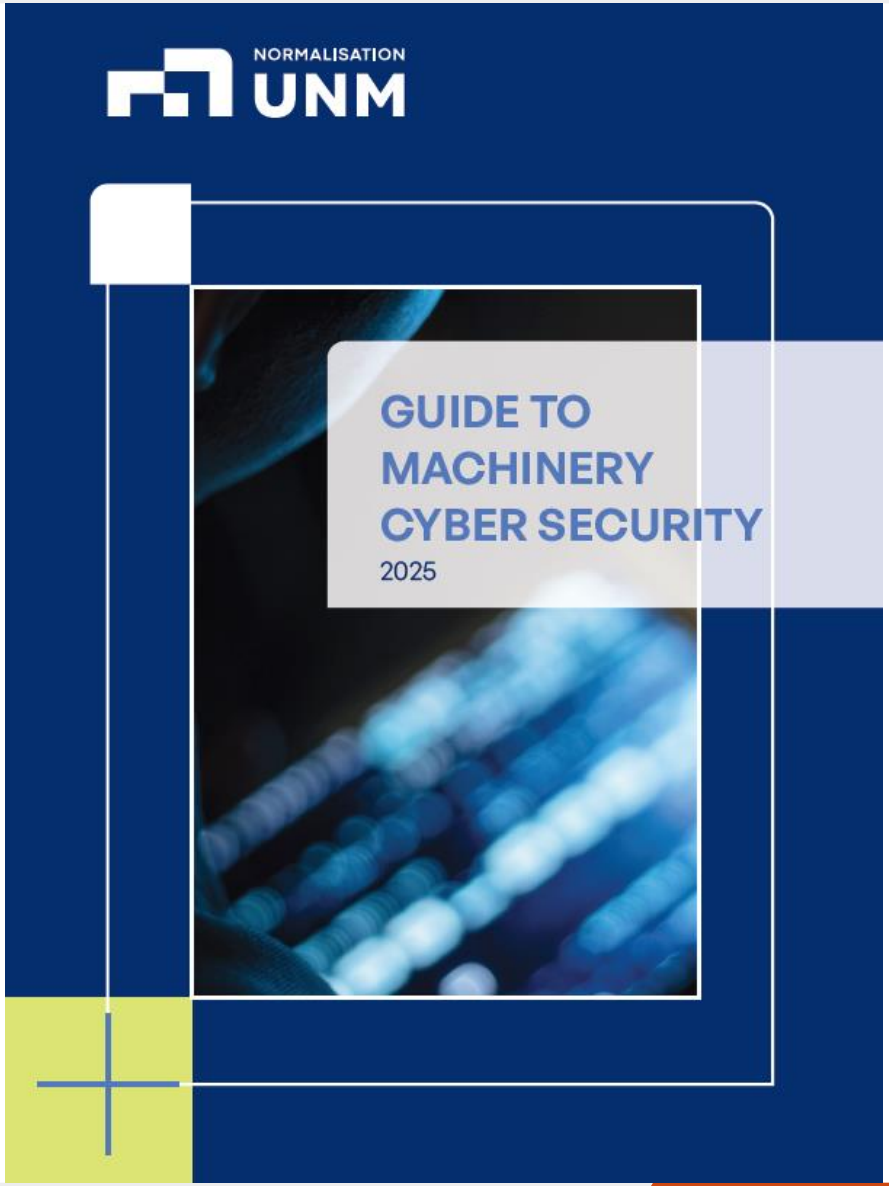
UNM - Guide to machinery cybersecurity - English version (https://ressources.unm.fr/guide-to-machinery-cybersecurity-2025)

Scope of the UNM guide

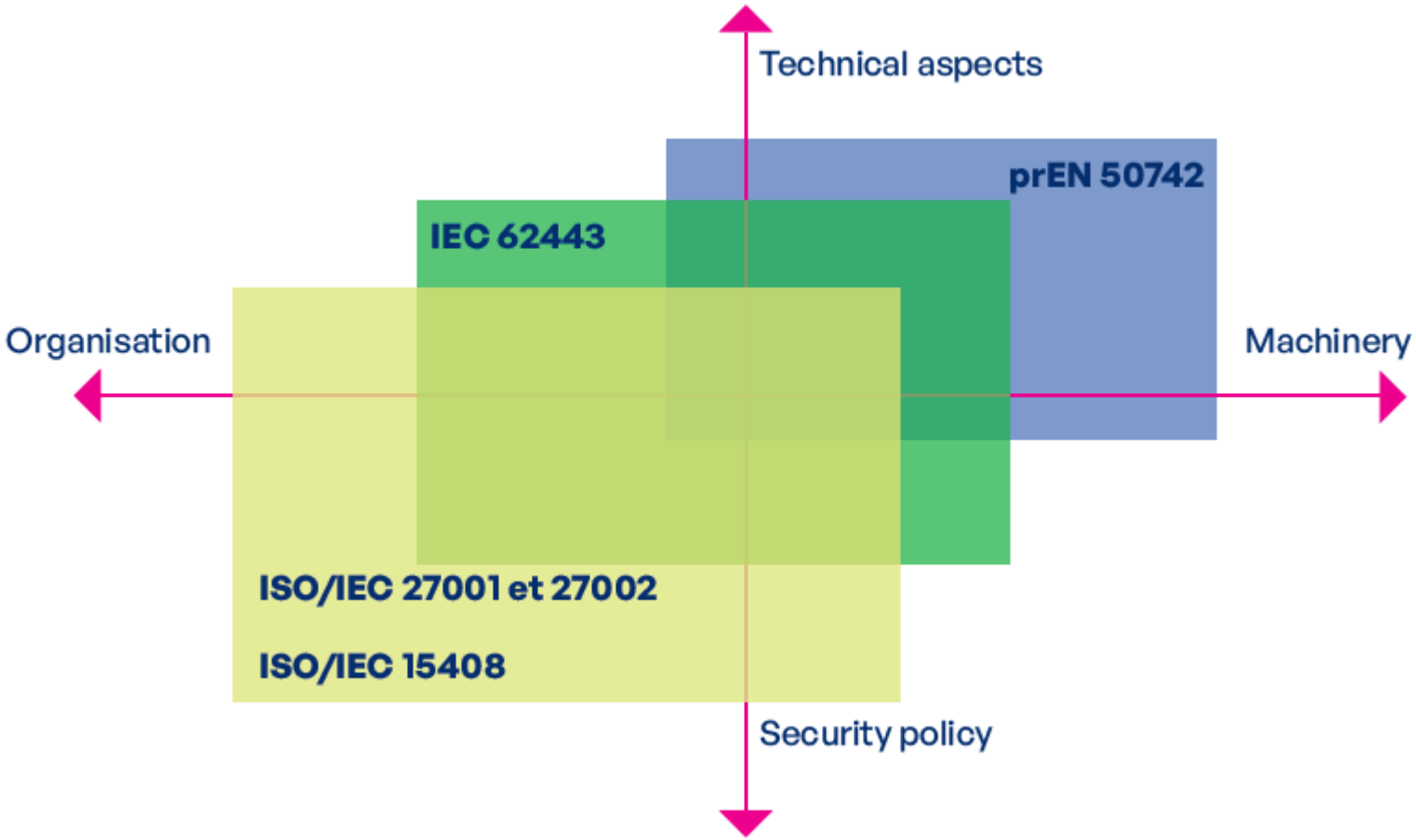
Giving a global insight into the cyber security aspects for designing machinery control system

Contents

- **Basic terminology**
- **Related standards**
- **5 steps method**



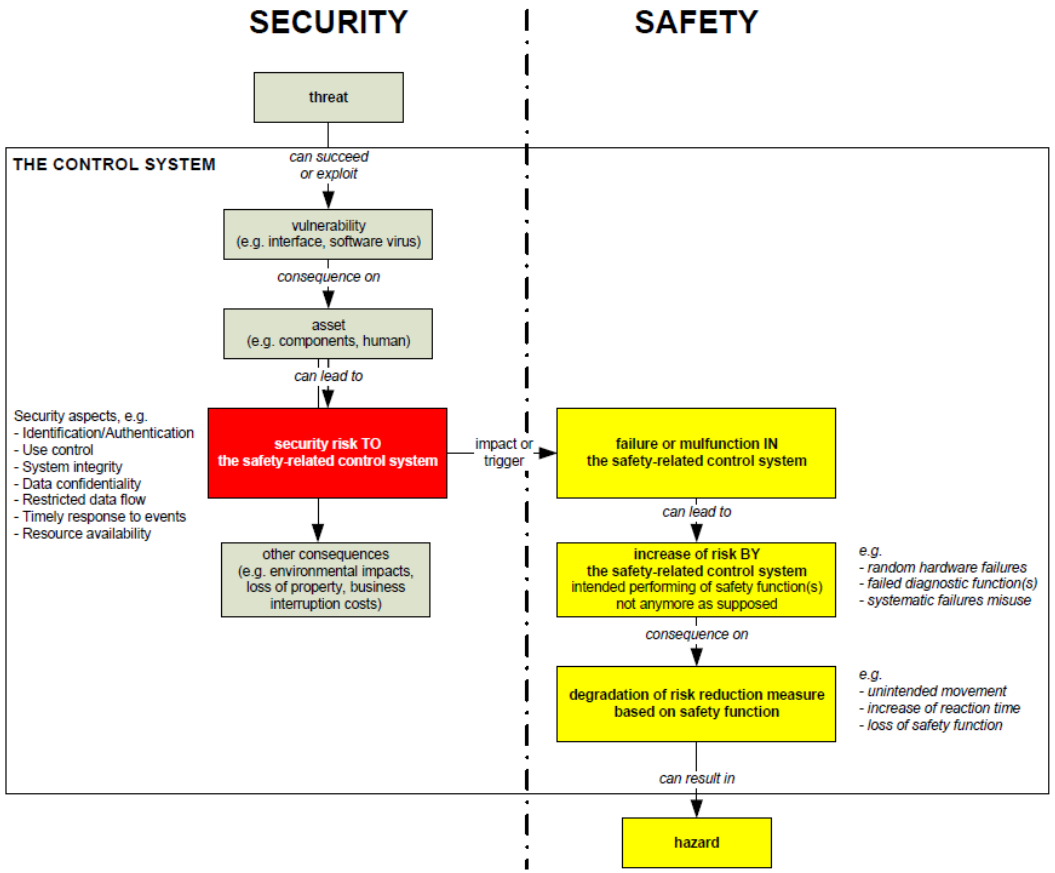
Corpus of international digital security standard



Links Security & Safety

IEC/TS 63074:2023

Security risks to safety-related control systems

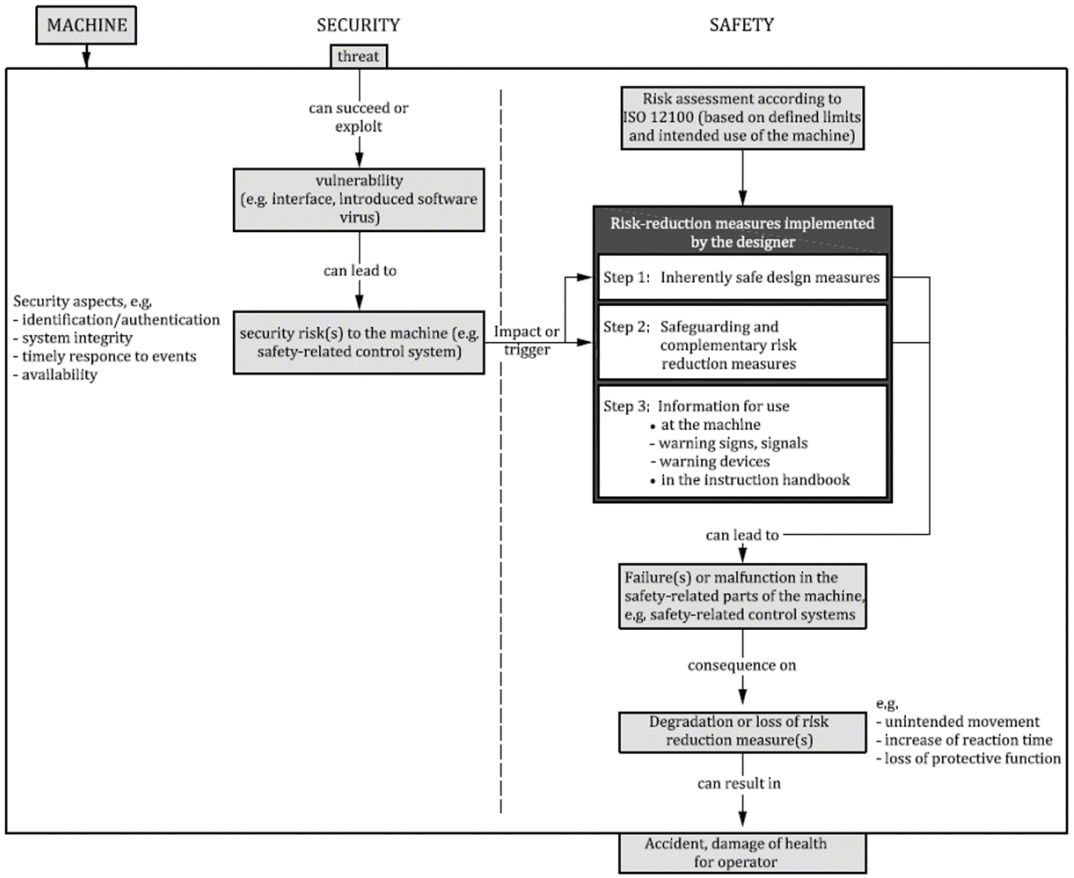


Links Security & Safety

ISO/TR 22100-4:2018

Security risks to safety-related control systems

Impacts on risk reduction measures implemented by designer



UNM Guide


What are the dangers?
1
Refer to ISO 12100
What type of exposure is expected (physical access, connectivity, etc.)?
2
Define the limits of the cyber environment to establish the chain of trust
What will the impact be on human safety and the safety function?
3
Define the threat scenarios
How can access be eliminated or protected, and how can operations be recorded?
4
Eliminate any known vulnerabilities
What information is required to use the machinery safely?
5
Define the instructions
?
Safety of machinery expert
Cybersecurity expert

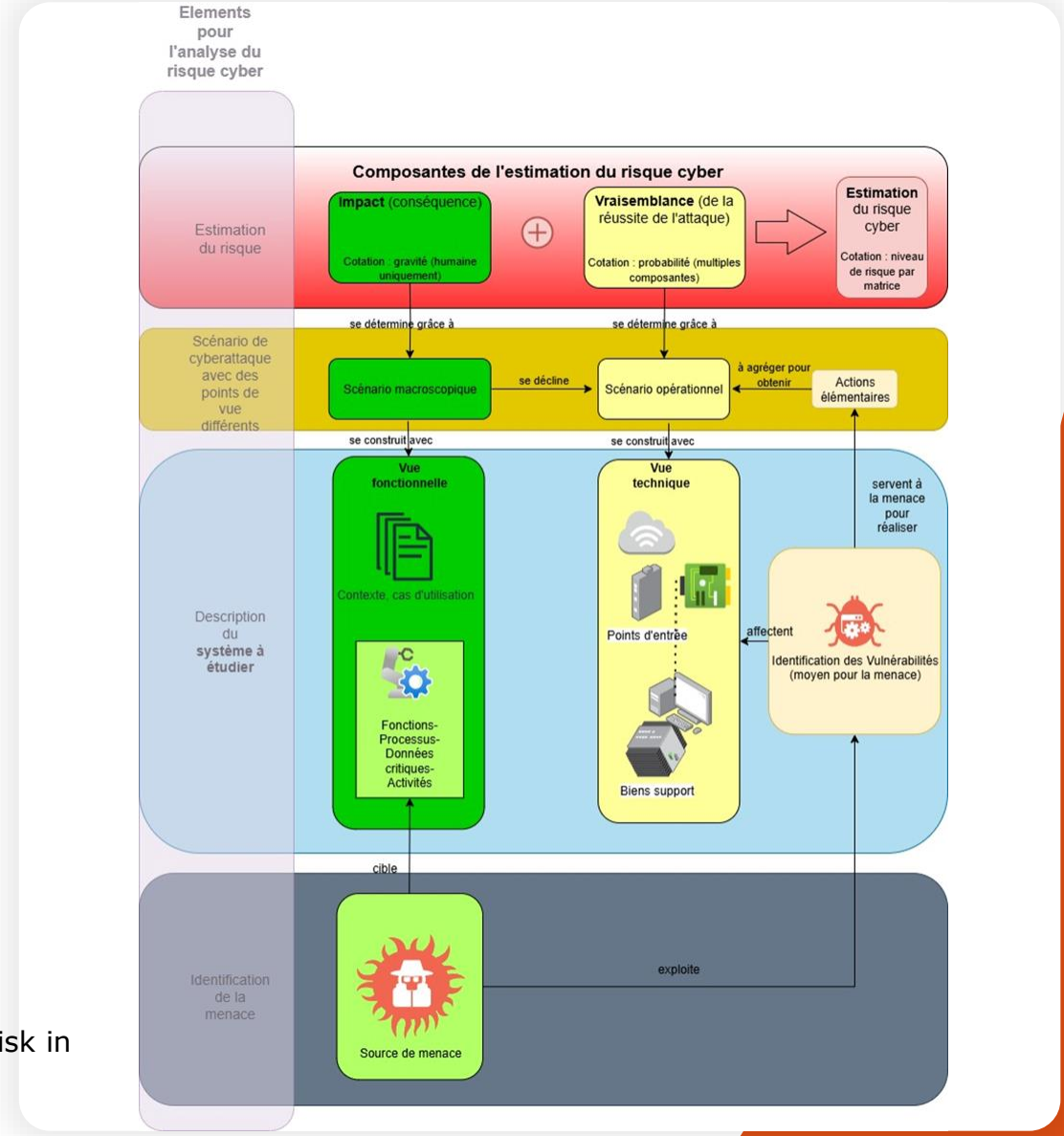
Work in progress @INRS

Making cyber risks accessible to OSH expert

Explain terms and concepts

Link between IT and OT

How conduct cyber and machinery risk assessment?



Lamy, P., & Flaus, J. M. (2026). A method of cyber risk assessment for occupational risk in machinery. International Journal of Occupational Safety and Ergonomics, 1–16. https://doi.org/10.1080/10803548.2025.2595860

03

AI in machinery

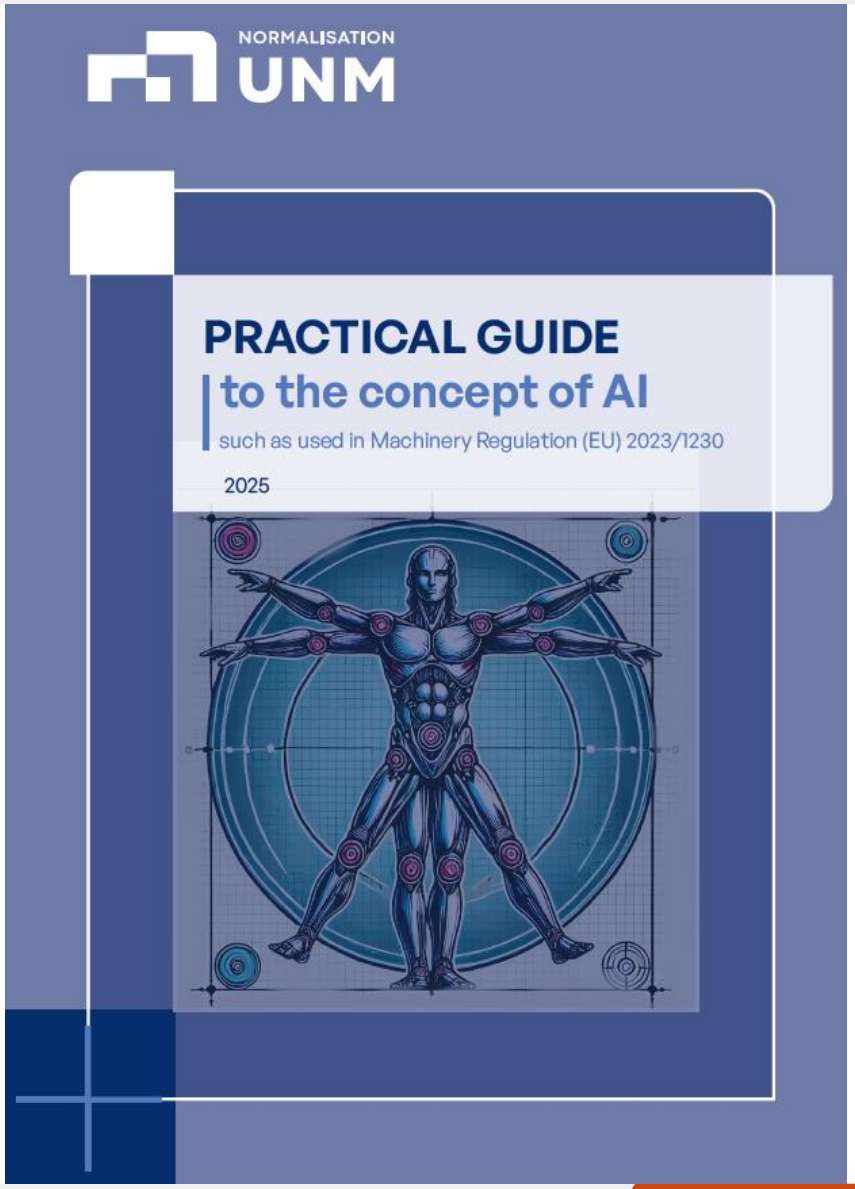
Resources

UNM Guide AI 2025 - English version (https://ressources.unm.fr/guide-AI-and-machine-safety-2025-english-version)

Scope of the UNM guide

Machinery Regulation (EU) 2023/1230, includes a new set of requirements relating to systems with self-evolving behaviour using machine learning approaches.

This guide provides a clearer insight into these systems and their limitations in compliance with safety principles.



« Basic » terminology

The term «artificial intelligence» refers to both an area of study within the field of computer science and a type of computer program.

The common denominator among programs named «AI» programs is that they have not been written by a human, but have been «self-generated» by an algorithm.

This type of program is called an «AI system» in ISO/IEC 22989:2022 «Information technology - Artificial intelligence - Artificial intelligence concepts and terminology».

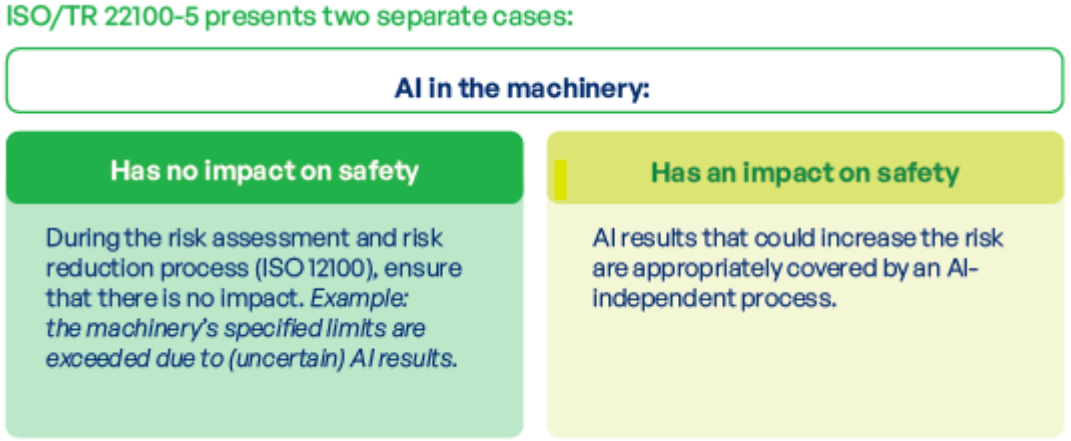
Two uses for this type of program are classed as AI:

- **Model training (phase for automatically generating the program),**
- **Use of the program (also known as the «inference» phase)**

Implications of machine learning

ISO/TR 22100-5:2021

This document does not address safety systems with AI, for example, safety-related sensors and other safety-related parts of control systems.

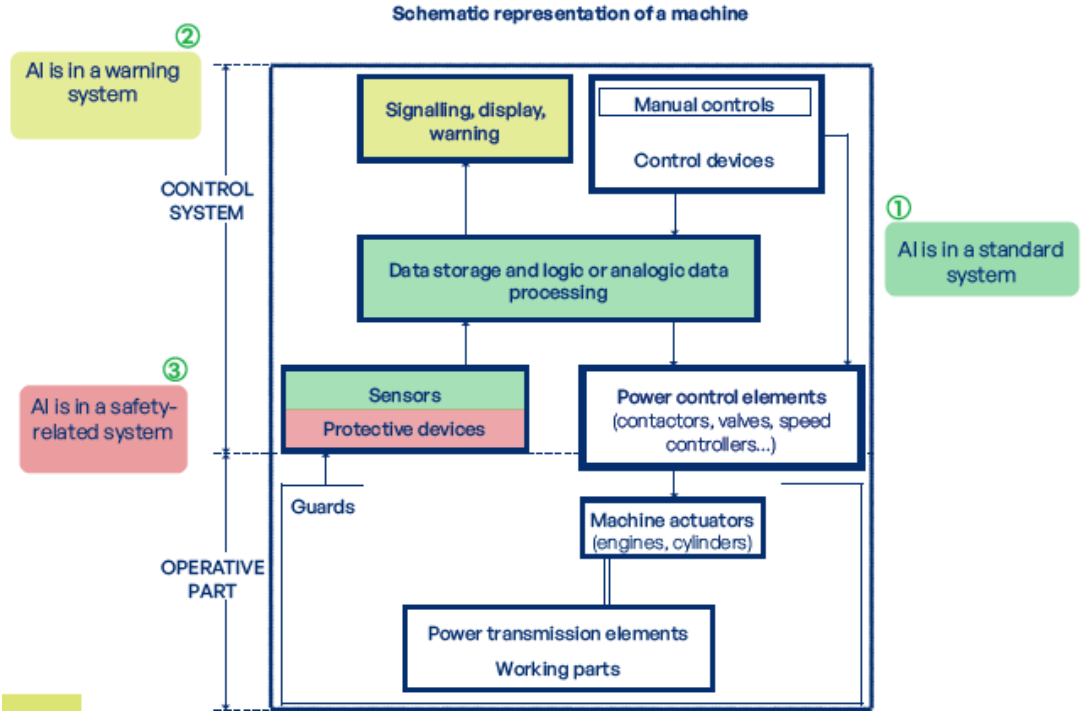


AI’s location within the control system

Using schematic representation of a machine from ISO 12100

The impact of AI on machines depends on its location within the control system of the machine.

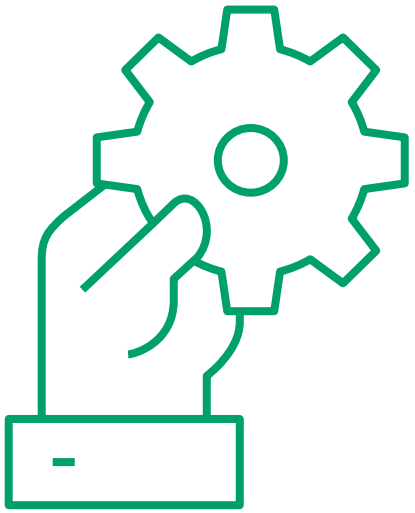
Three specific locations are highlighted to show these different impacts.

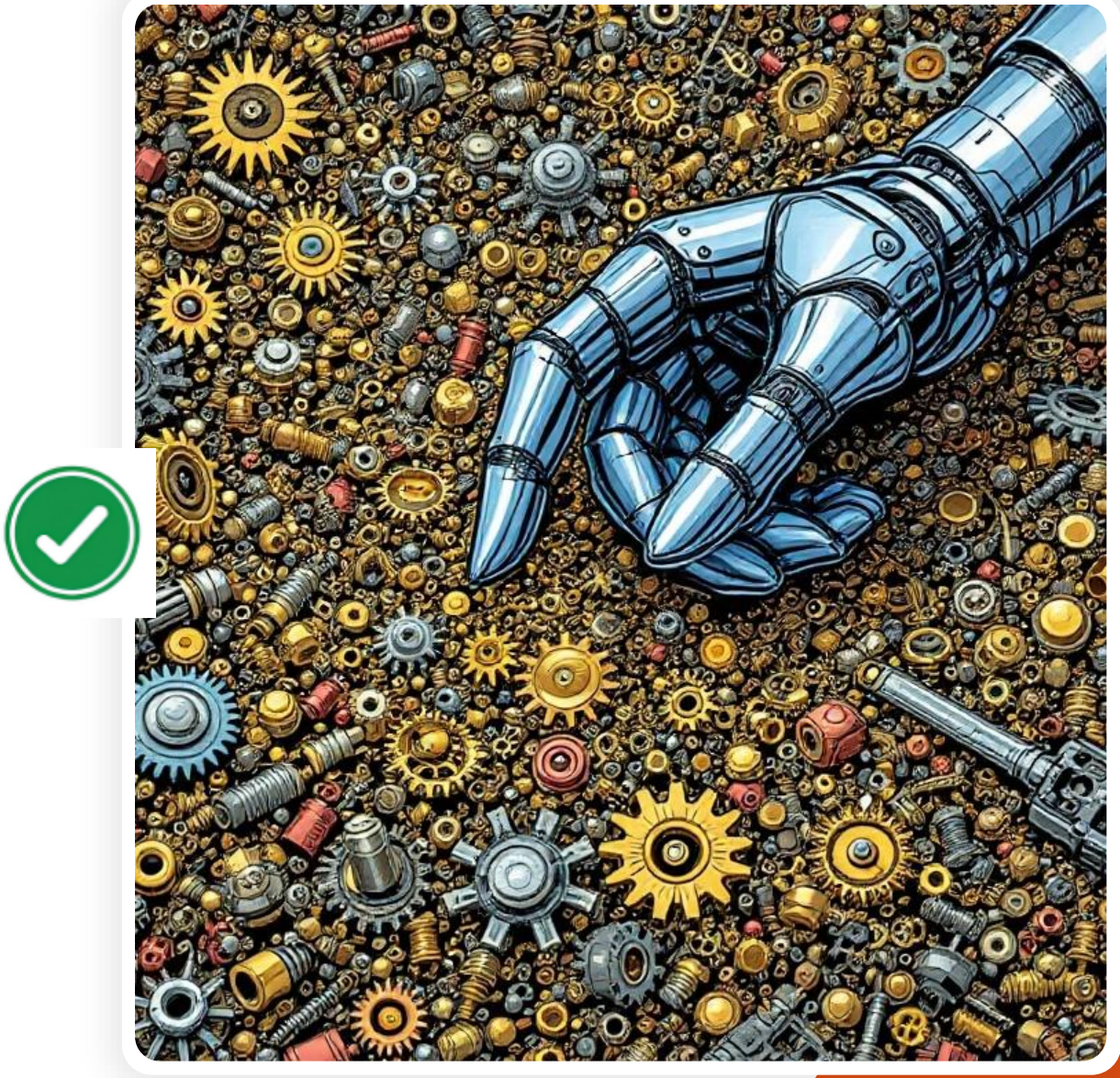


7.3 Use case I

AI system used to perform a standard function in the machinery.

Bin picking robot in the manufacturing industry





7.3 Cas d’usage II

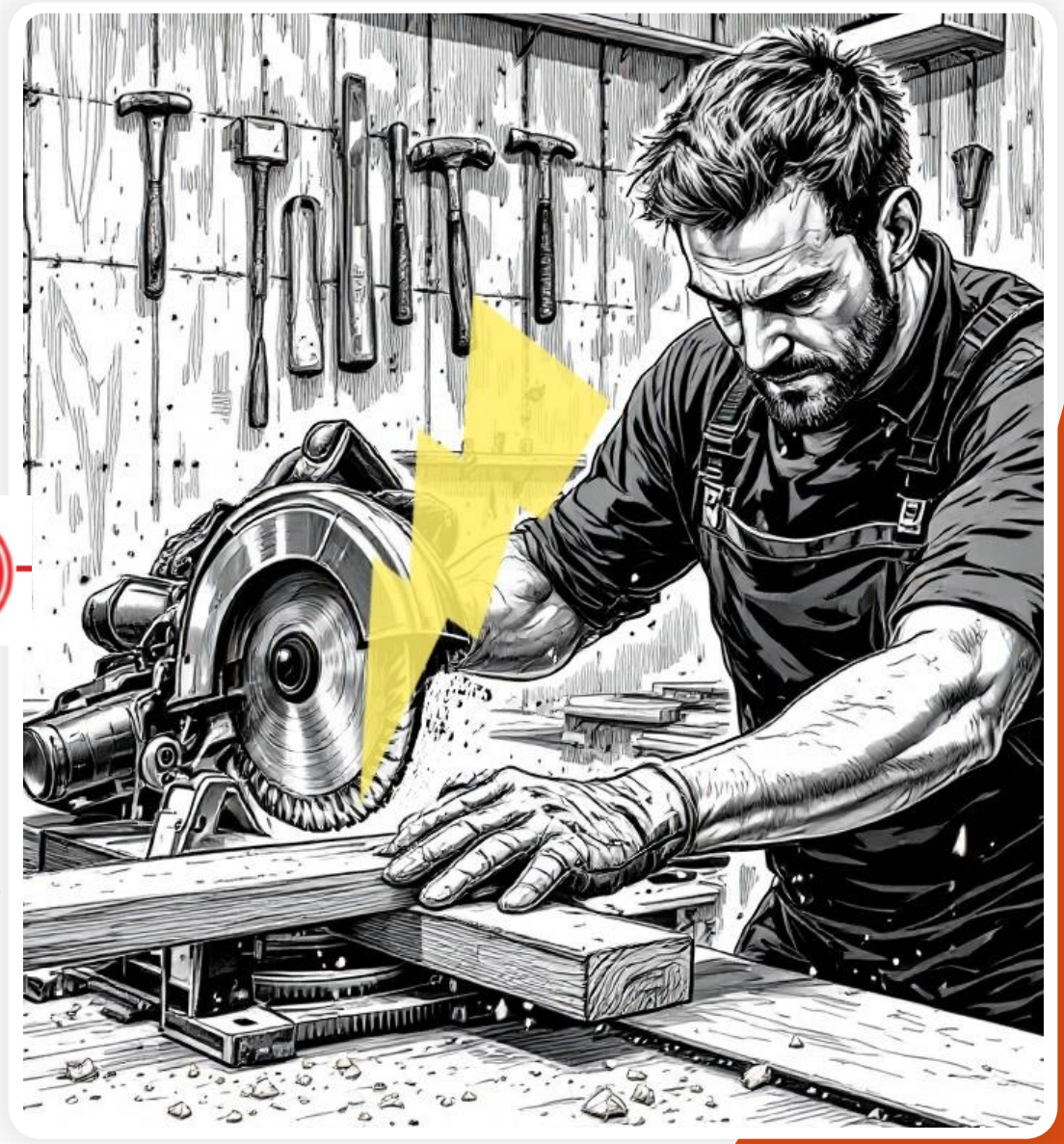
AI system used to perform a warning function

Warn drivers when people stray into their vehicle’s path

7.3 Cas d'usage III

AI system designed to perform a safety function

Retract a table saw blade when the operator's hands approaches it



ISO 19085-5 introduces the notion of AIMS (*Active Injury Mitigation System)* using (or not!) AI
system that detects contact or proximity above the machine table between a rotating saw blade and parts of the human body (e.g. finger, hands) and reacts to mitigate an injury.

BUT which **is not a protective device**

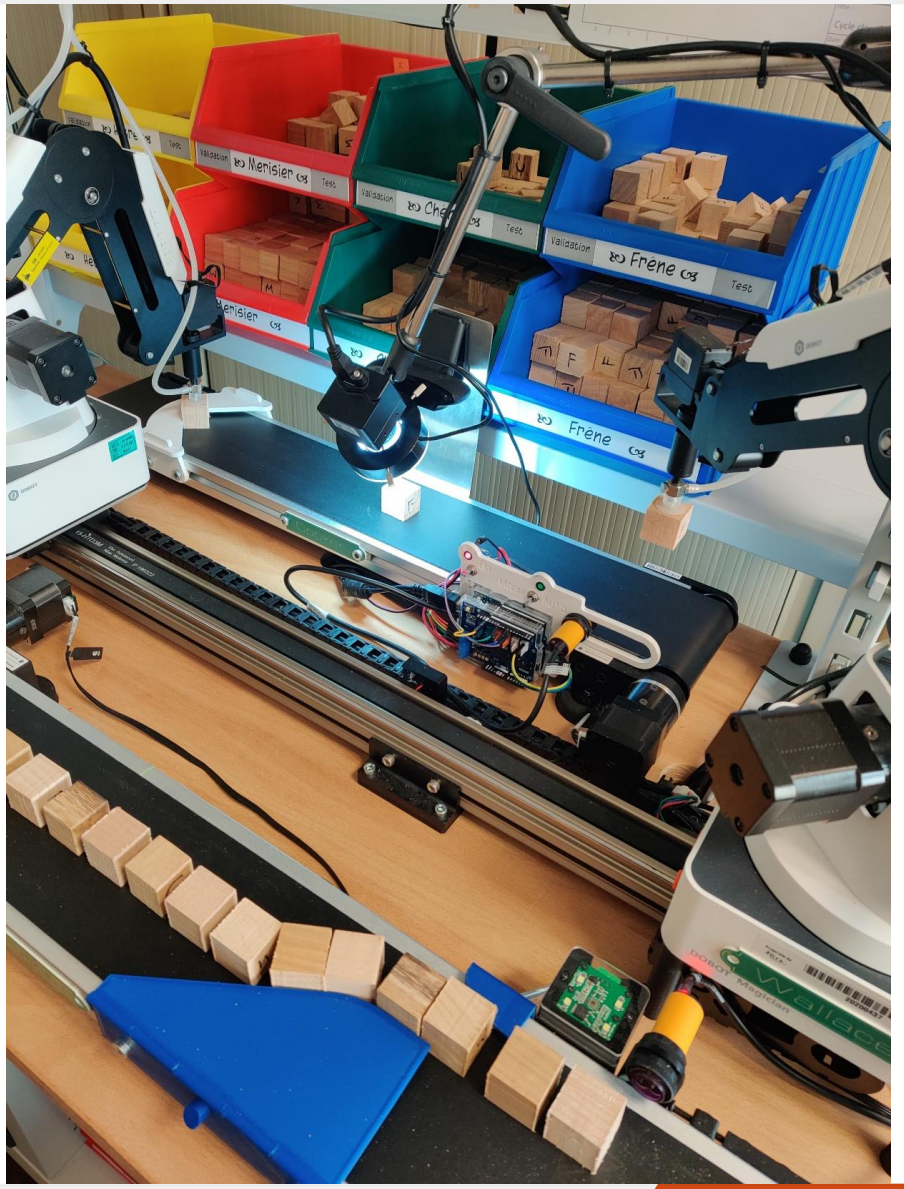
Studies @INRS

Features of machines using AI

Design cycle - Model training phase

The decision-making process is inexplicable

No determinism at the macro level



Sarrey M. (2024). How can functional AI be safely integrated into a machine? Proceedings of SIAS 2024, 12-13 June 2024, Tampere (Finland), https://www.automaatioseura.fi/site/assets/files/4501/sias_2024_paper_12.pdf

Determinism

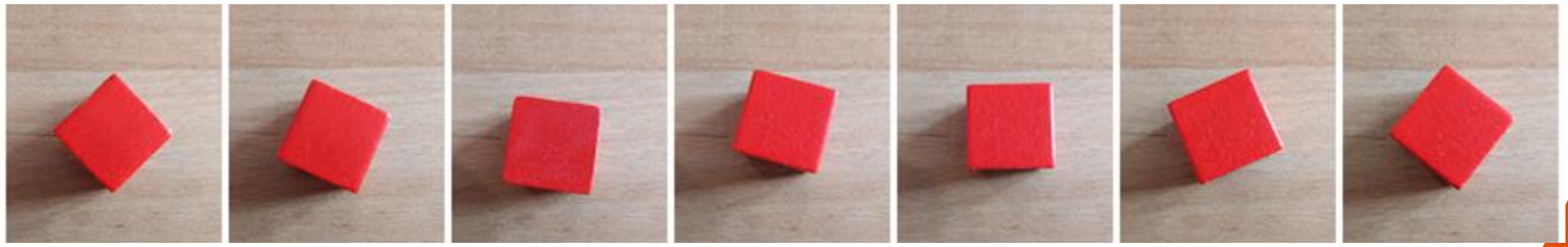
For the automation, determinism is the ability of the system to produce at anytime the same outcome with the same input dataset.

ML algorithm is deterministic but using AI system produces two issues:
The behaviour of the system will change after a new training.
The difficulties to present the same input dataset twice.

The next seven photos show the inputs dataset, this red cube is shot on the same stage with the same environment.

For the process, it is the same object, however, for the computer vision software, it is seven different datasets.

Even if these differences are minimal, the outcome can change.



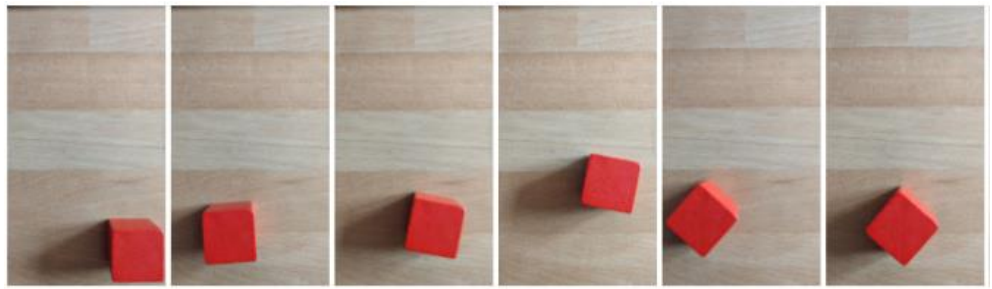
Seven shots of one red cube

Opacity and explicability

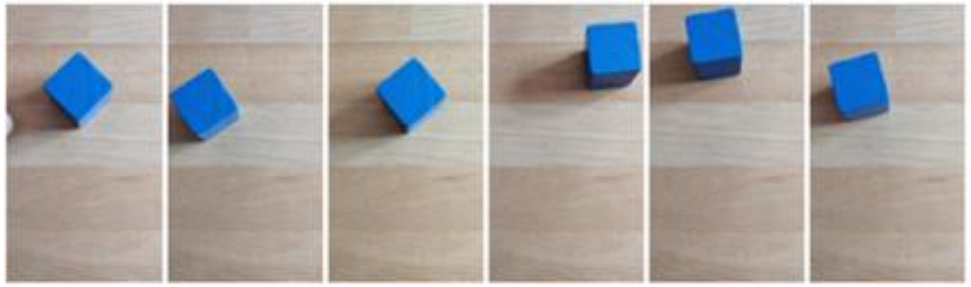
The problem of inexplicability makes difficult to train the model and hides eventual bias in the training data bank.

ML is based on a mathematical theory. By principle, each step of calculation is transparent and re-executable.

Most advanced ML software (like Deep Learning) uses millions of parameters in their neural network: due to the number of parameters, the outcomes become inexplicable.



The model trained with the images bank above can predict that following cube is red:



and that one is blue:

04

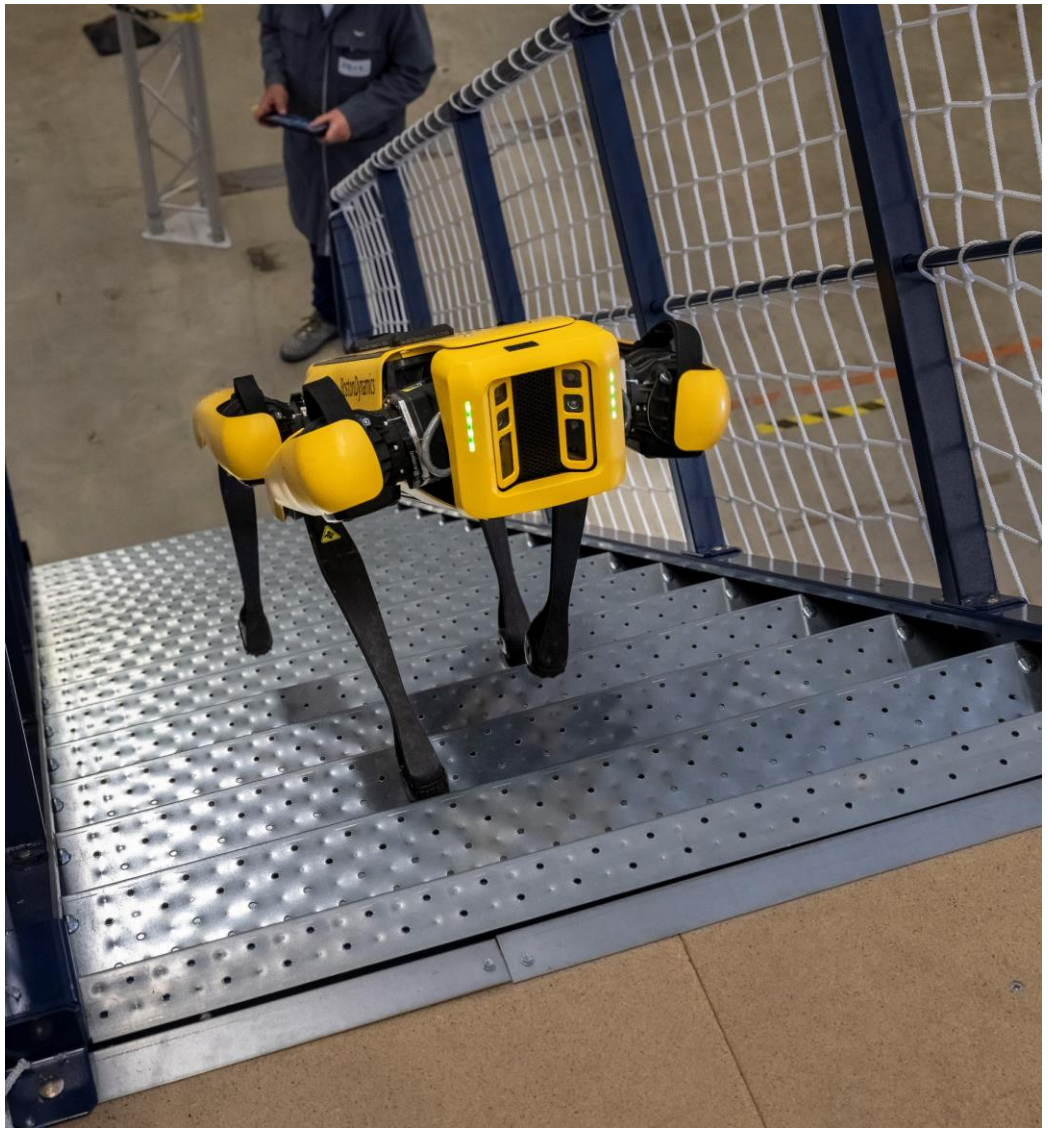
Any other challenge?

Prospects

Mobile robotics / Humanoid

Combining Cyber & AI challenges

Robot Optimus de Tesla, juin 2025
© Giovanni Cancemi / Shutterstock



Thank you for your attention

Our job:
making yours safer

www.inrs.fr