Safety considerations in autonomous products

Charalambos Freed

Vice President Nilfisk A/S

Member IEC ACOS TF
Collaborative Safety

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS
SC 42 – Artificial Intelligence

Introduction

From manual to autonomy

The evolution in technology and introduction of intelligent systems leads to new solutions which need a framing from safety perspective to create trustworthiness.

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS
SC 42 – Artificial Intelligence

Nilfisk – Charalambos Freed

- Vice President – Head of Standardization and Government Relations
- Chairman Technical Committee EUnited Cleaning
- Chairman Arbeitskreis Technik VDMA FV Reinigungssysteme
- IECEX Management Committee – Head of Greek Delegation
- Member WG Testing Bundesverband Deutsche Industrie
- IEC Member ACOS TF Collaborative Safety
- IEC Secretary SC 61J
- IEC Convenor TC 31 JMT62784
- IEC Secretary TC 61 WG44
- IEC Secretary TC 61 WG49
- IEC Convenor SC 61J MT 03
- IEC Convenor SC 59F WG 06
- Chairman CSA C234
- CLC Convenor TC 61 WG 6 + WG 10
- CLC Convenor TC 59 X WG 06-03+04
- CLC Convenor TC 31 WG 24
- Issue Manager EN 60335-2-67, -68, -69, -72, -79, EN 62784
- DKE Convenor AK 513.7.10
- IEC 1906 Award Winner

Environment / Circular Economy

Safety ⟷ Performance

- Hazardous substances
- Waste
- […]

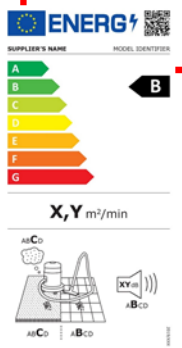
Partially

CE

Ecodesign Directive

- Repair
- Recycle
- Refurbish
- Remanufacture
- Upgrade
- Add. Durability

[…]



CE

Safety

Safety ⟷ Performance

Directives:

- Machinery
- Product Liability
- Explosive atmosphere
- Outdoor Noise

[…]

CE

Digitization/Digitalization

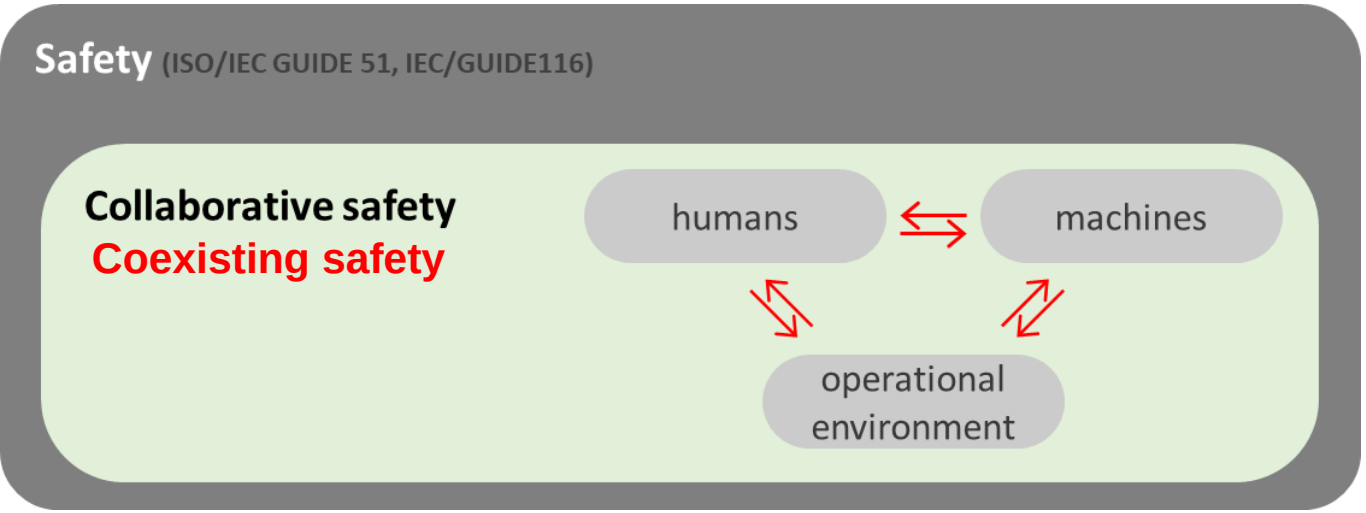
Safety ⟷ Performance

- Cybersecurity Act
- General Data Protection
- Artificial Intelligence
- IoT modules in machines
- […]

OT vs IT

- Machine Safety
- Cloud Data

New trends impacting safety



- Intelligent systems: primary drivers of digital transformation.
- Collaboration vs Coexistence: safety considerations
- Concerns: privacy, data integrity, safety, security, transparency and trustworthiness of new technologies.

Projects related to collaborative safety
ACOS 2nd survey among safety related TCs

- Interest
  - Coexistence first + collaborative safety in certain applications; assisted remote operation, automated decision making
- Challenges
  - Hazard-based design, self-detection of faults
  - New user/operator training information including public users
  - Maintenance; human factors
  - Risk management during use phase
  - Adaptation of functional safety technics
  - Identify applicable machine learning technics including statistics
  - Conformity assessment

ACOS task force
SMB decision 170/16

- Assess the evolution of technical development and standardization in this field
- Perform a gap analysis of any missing work
- Recommend to SMB future standardization work and roadmap
- Collaborate with ISO in this area

IEC SC 61J: commercial/industrial cleaning equipment

Transformation of machine: from manual to autonomous mode

manual

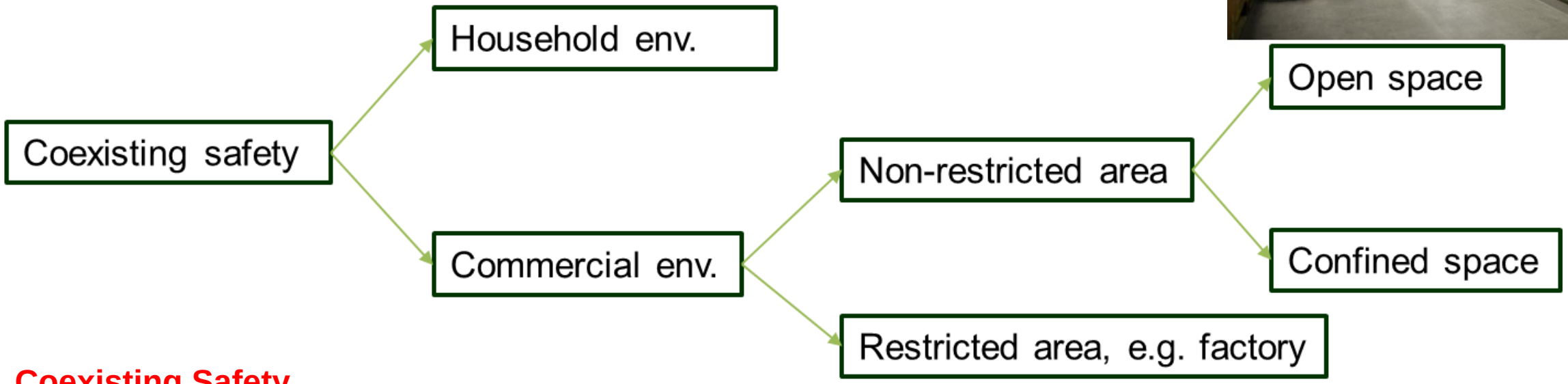
„magic addition“

autonomous

„Magic ingredients“

Parameter		
	Manual	Autonomous
Electrical and mechanical safety	Y	Y
EMC requirements	Y	Y
Attended machine	Y	**N**
Additional requirements as unattended machine on • motor, • plastics, • hardware, **software**, • environment.	-	Y
Obstacle and drop-off detection	-	Y

Environment: coexisting safety



Coexisting Safety

machine ensured safety, where humans share the same physical space with automatic / autonomous machines (robots, mobile robots), but generally act independently or with different tasks.

Collaborative Safety

machine ensured safety, when humans perform intended mutual actions together with automatic / autonomous machines (robots, mobile robot) to accomplish a common task

Environment: coexisting safety

- Commercial area: open space, dynamic environment, vulnerable people
- Person stands/lays/runs in front of machine.
- Person climbs onto the operator platform and/or pushes buttons.
- Person approaches from side.
- Machine heads towards drop-off.

IMPORTANT:
Intentional movements of persons towards the appliance in order to harm themselves, is **not covered.** The result would be a static appliance…

Route on getting the safety up and running

Liaison Officer IEC TC 61 → ISO TC 299: Mr. Dejun MA (CN)
Liaison Officer IEC SC 61J to ISO TC 299: Mr. Charalambos Freed (GR)

IEC TC 61 WG 44: Safety of robots for household and similar use
Chair: Mr. Dejun MA (CN); **Secretary:** Mr. Charalambos FREED (GR)
Standard: Draft based partially on IEC 63327

IEC SC 61J MT 3, IEC 63327: Safety standard for autonomous commercial floor treatment machines
Chair: Mr. Charalambos FREED (GR)
Secretaries: Mr. Kenneth WILLS (US); Mr. Leonard LETEA (CA)
Standard: IEC 63327; based on CSA/ANSI C22.2 No. 336-17

CSA C234: Safety electrically operated appliances
Chair: Mr. Charalambos FREED (CAN)
Standard: CSA/ANSI C22.2 No. 336-17

Commercial environment

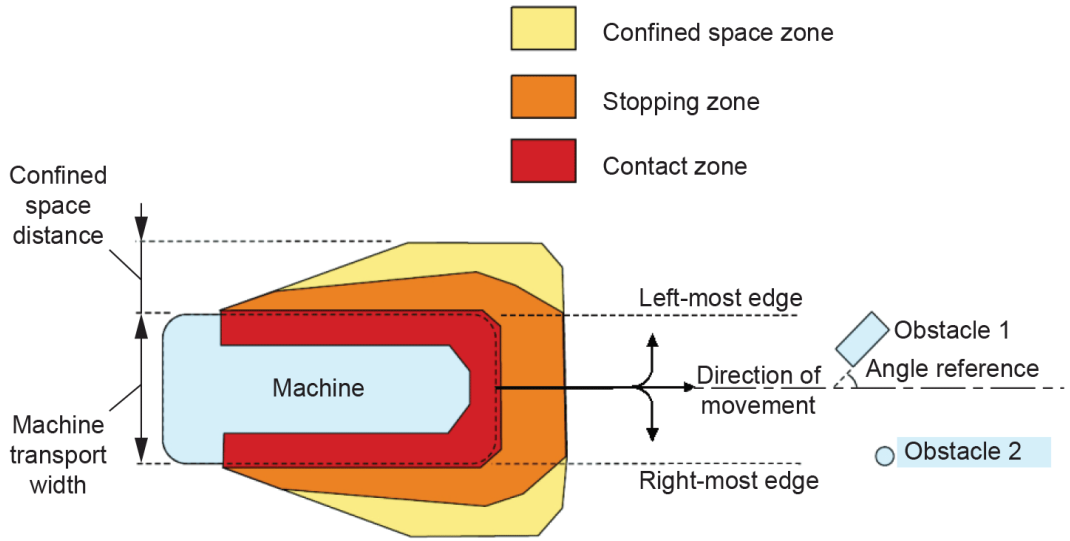
Type and purpose of safety-critical function (SCF)	Minimum required performance level (PL) as described in ISO 13849-1	
	Type 1 machines	Type 2 machines
Drop-offs detection	PL = d	PL = d
Prevent intrusions into stopping/contact zones to prevent crushing + collision	PL = b	PL = d
Prevent exceeding autonomous mode speed	PL = b	PL = d
Provide locked state of drive wheels	PL = b	PL = b
Provide desired (emergency) switch-off	PL = b	PL = c
Provide desired stop category 0, 1, or 2	PL = b	PL = d

type 1 machine: velocity max. 3 km/h, height max. 50 cm and weight max. 20 kg
type 2 machine: other than a **type 1 machine**

PL and definition
ISO 13482: Robots and robotic devices — Safety requirements for personal care robots

Tests

Autonomous test – start appliance



Starting of motor-operated appliances

- Initial start-up/restart: passcode/key-protected control device, or equivalent.

General conditions for the tests: Obstacles detection in direction of motion

- Obstacles covered in black felt/coarse fabric. Reflectance between 5 - 10%:
  - obstacle 1 - cylinder Ø 200 mm + length of 600 mm, placed horizontally; obstacle 2 - cylinder Ø 70 mm + height of 400 mm, placed vertically.
- Lighting levels between 100 - 1000 lx.
  - In alignment with IEC TS 61496-4-2 and /-3 - Safety of machinery – Electro-sensitive protective equipment

Autonomous test – drop off

- Protection against drop-offs, e.g, staircases, unprotected drop-offs, in all travel directions.
- Test surface 11 ± 1 cm above adjacent surface.
  - Test conducted under most unfavourable conditions, based on sensor positions,
    - both starting from rest and in motion towards the abrupt surface elevation change.

Autonomous test – speed and stopping distance

Speed

Autonomous mode, open space environment, max. 6 km/h; confined space environment, max. 4 km/h.

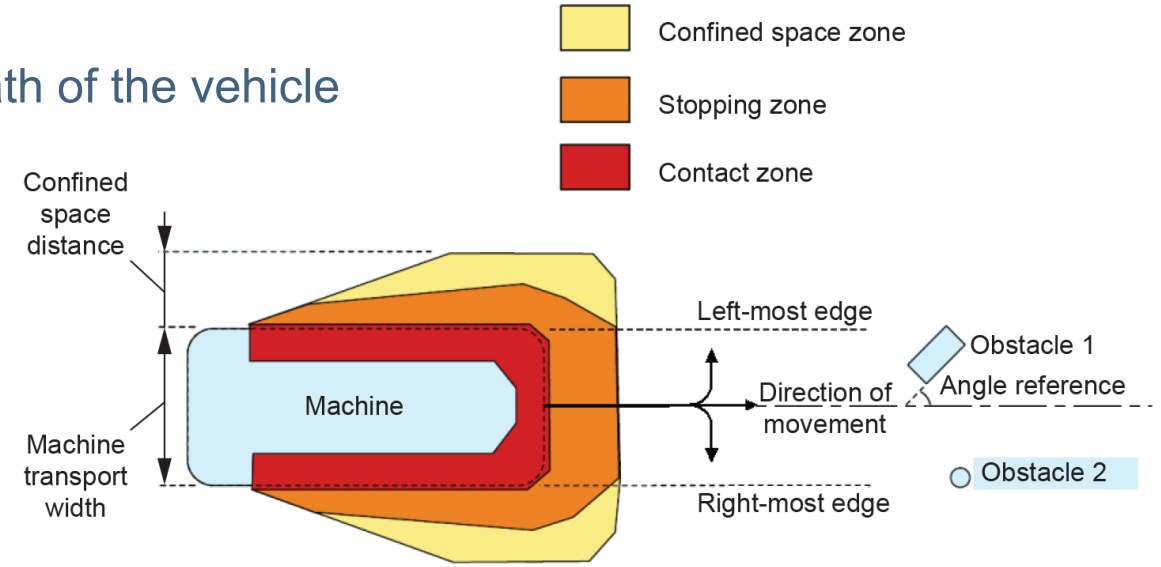
Stopping Distance

Measured with maximum rated automatic speed of machine in direction of test.

NOTE Stopping distance is based on a reaction time below 0,5 seconds.

Autonomous test – obstacle detection

- **Initial start-up**
- Both obstacles in **contact** with machine in potential areas of motion → avoid contact.
- Objects **entering stopping zone**: either stop category 2 or obstacle avoidance
- Test obstacles in front of the machine; speed: Confined space + rated autonomous.
- Test obstacle 1: Laying down at 0°, 45°, and 90° to the path of the vehicle
  - @ > safe stopping distance
- Test obstacle 2: Set vertically at angles as above.
  - @ safe stopping distance range

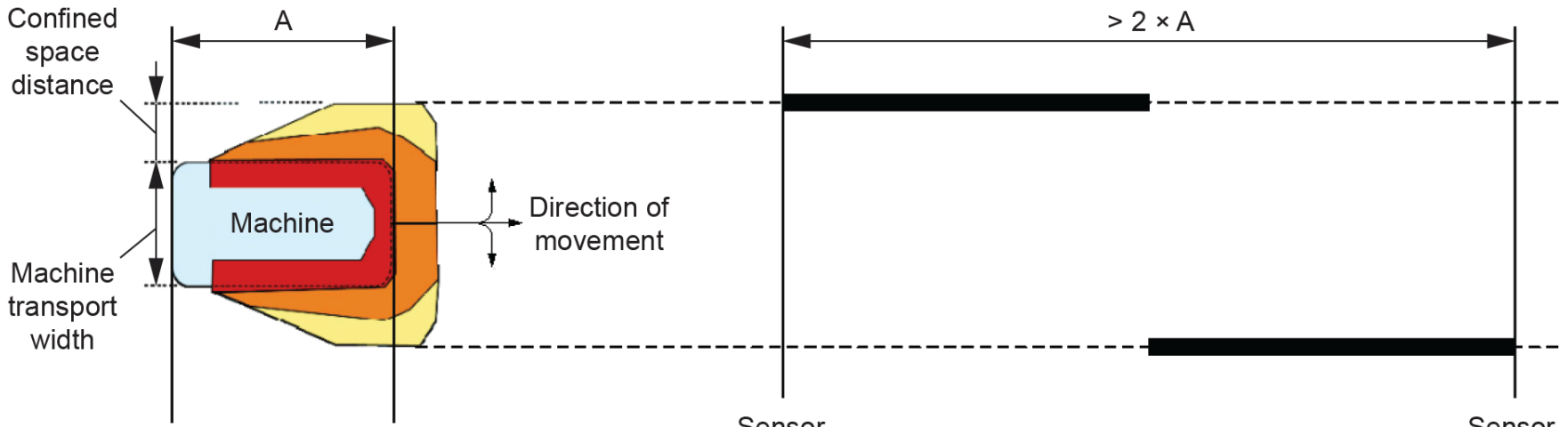


(illustration purposes only)

IEC

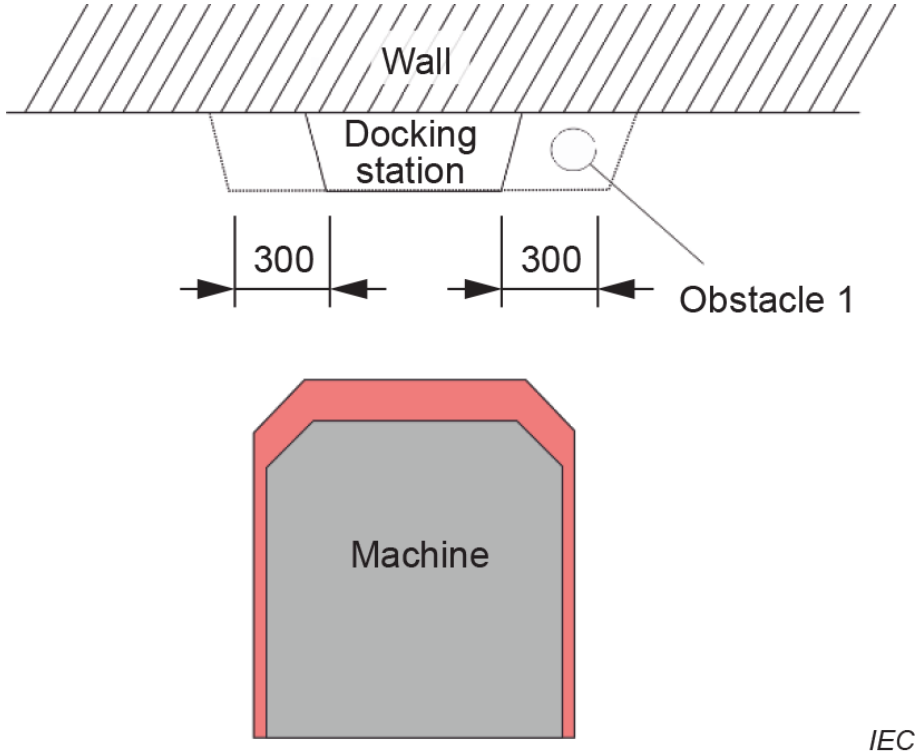
Autonomous test – confined space

- Two continuous walls or obstacles, each with a minimum length equal to the machine transport length and a minimum height of 1 m.
- Sensors are allocated at each end of the test area to measure the start and finish of the machine traversal (speed).
- Machine (GVW rating) moves with maximum open space speed and enters the confined space test area.
- Measured over three successful speed measurements.



IEC

Docking Station



IEC

Test setup:

- Modification of IEC 60335-1;
- Safety distances given in ISO 13857:2019
- During Docking process: acoustic or visual warnings,
- Velocity max. 0,05 m/s,
- Max. 0,2 m in linear direction to complete docking process,
- equipped with a detection system
- Back-siphonage: modification of IEC 61770;

Adding more „intelligence“

- Adding Artificial intelligence to enhance productivity / safety and reduce design complexity
- However,
  - Method needed to assess dependability to receive transparency and predictability of algorithms

Software and communication

- **Software** architecture, safety, error avoidance, updates, security/data integrity, remote communication →
  - **Annex R and U** with additional references to applicable standards
- **Attended vs unattended** appliances: additional safety requirements

IEC 60335-1

Edition 6.0 2020-09

Annex R
(normative)

Software evaluation

Annex U
(normative)

Appliances intended for remote communication through public networks

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS
SC 42 – Artificial Intelligence

IEC 60335-1 - excerpt

- 22.46 If programmable protective electronic circuits are used to ensure compliance with this standard, the software shall contain measures to control the fault/error conditions

  → Annex R

- 22.62 Remote communication through public networks shall not impair compliance with this standard.

  → Annex U

IEC 60335-1 - excerpt

Annex U
(normative)

Appliances intended for remote communication through public networks

The measures given in this annex are intended to avoid unauthorized access and the effects of transmission failures via **remote communication** through **public networks**, where compliance with this standard could be impaired.

However, in general, it does not cover aspects concerning confidentiality of data and consumer privacy.

IEC 60335-1 - excerpt

U.3.2 Remote communication shall be established, implemented and terminated by the appliance via software that provides

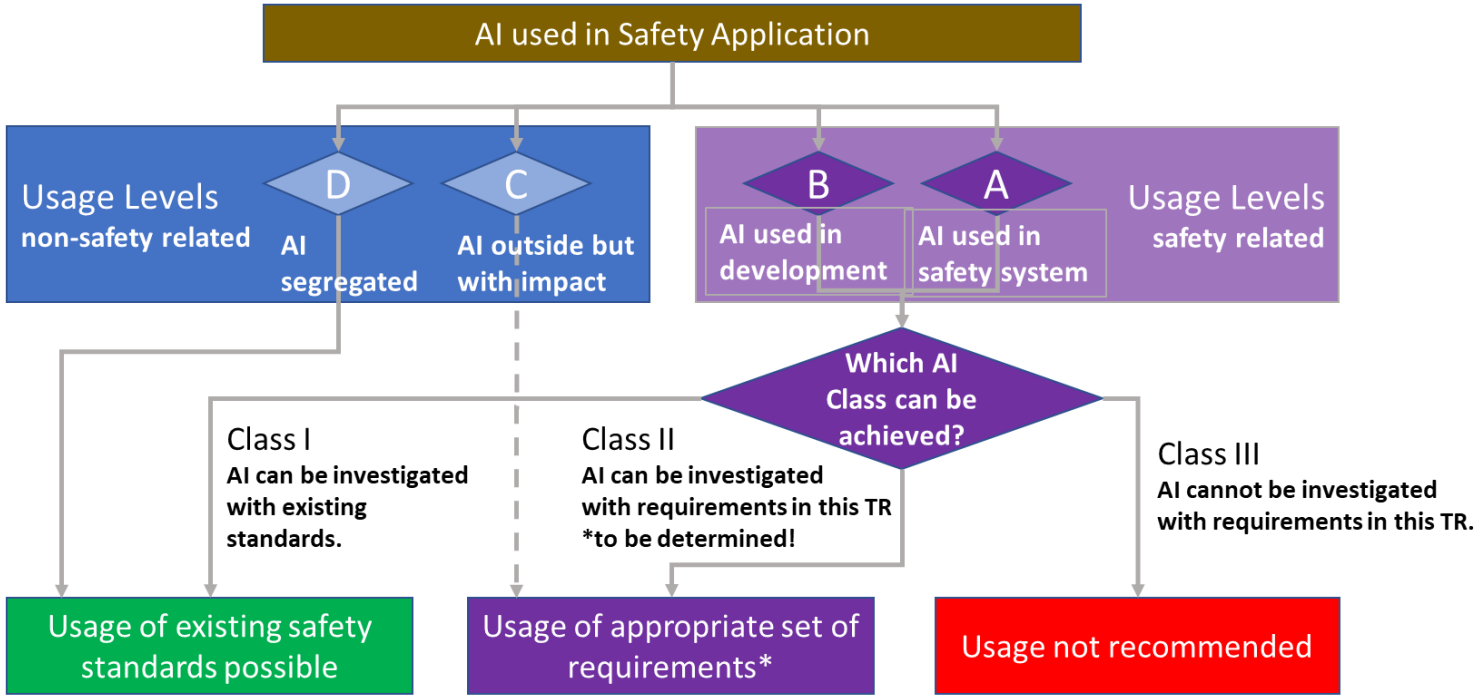
- data integrity protection concerning:
- data corruption;
- address corruption;
- wrong timing or sequence;

U.3.6 The safe operation of an appliance shall not depend on remote communication.

Compliance is checked by evaluation according to U. 3.2. In case of doubt, remote communication shall be rendered inoperative for the relevant tests of this standard.

Classifications

ISO-IEC TR 5469 proposes a classification scheme for AI used in safety related applications



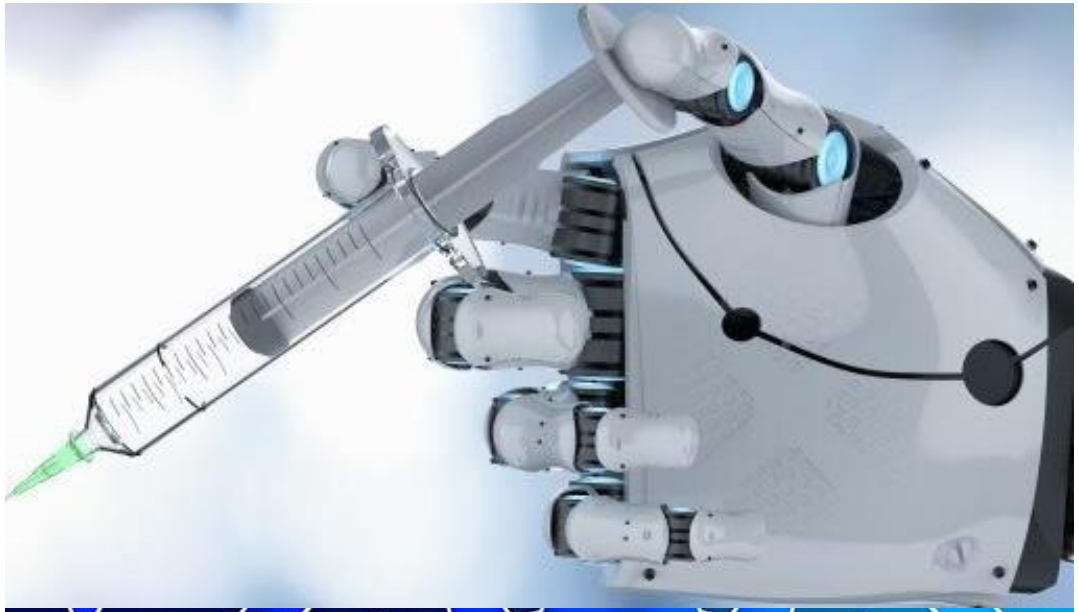
Important: The set of requirements for ISO-IEC TR 5469 will be new and independent.

Thank you

Charalambos Freed

cfreed@nilfisk.com

Nilfisk.com



ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS
SC 42 – Artificial Intelligence