SAFETY REQUIREMENTS FOR INDUSTRIAL AND SERVICE ROBOTS

Dipl.-Ing. Theo Jacobs
Fraunhofer Institute for Manufacturing Engineering and Automation (IPA)

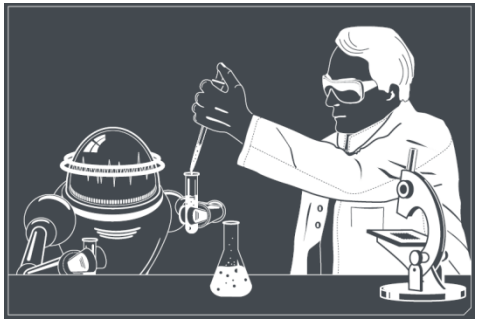
Fraunhofer IPA

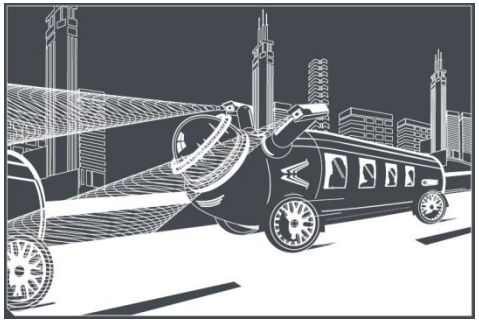
Agenda

- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Detailed requirements for industrial robots
  - Detailed requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

Why robot safety?

- Many robots have power to severely injure a human, especially by causing
  - Impact damage
  - Crushing
  - Clamping
- In many applications robots are supposed to work in direct proximity of a human
  - Collaborative work between human and industrial robot
  - Various service robot applications
    - Robotic co-workers
    - Household/personal assistants
    - Person transport robots
- Additional measures are necessary to prevent harm





© Strategic Research Agenda for Robotics in Europe

Why robot safety?

- The manufacturer of a robot is responsible for the safety of the machine
- Requirements in laws and standards for safe design have to be fulfilled
  - not only for robots that are sold as products
  - but also for robots permanently installed in laboratories
- For the development of a safe robot, the manufacturer should
  - be aware of his duties to reduce risks, to document the design process and to inform users about remaining hazards
  - consider safety issues as early as possible in the design process
  - choose applications with respect to the possibility to execute tasks reliably and safely

➔ Not everything that seems technically possible can be realized in a safe way

Agenda

- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Special requirements for industrial robots
  - Special requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

Safety standards …

- Application is voluntary
- Are written by representatives from industry, research, administrations, society
- Under the roof of a standardization organization
  - Global, e.g. ISO, IEC
  - Regional, e.g. CEN, CENELEC in Europe
  - National, e.g. DIN (Germany), ANSI (USA), etc.
- Reflect the current state of the technology
  - Existing, well-known products
  - Established measures for increasing safety

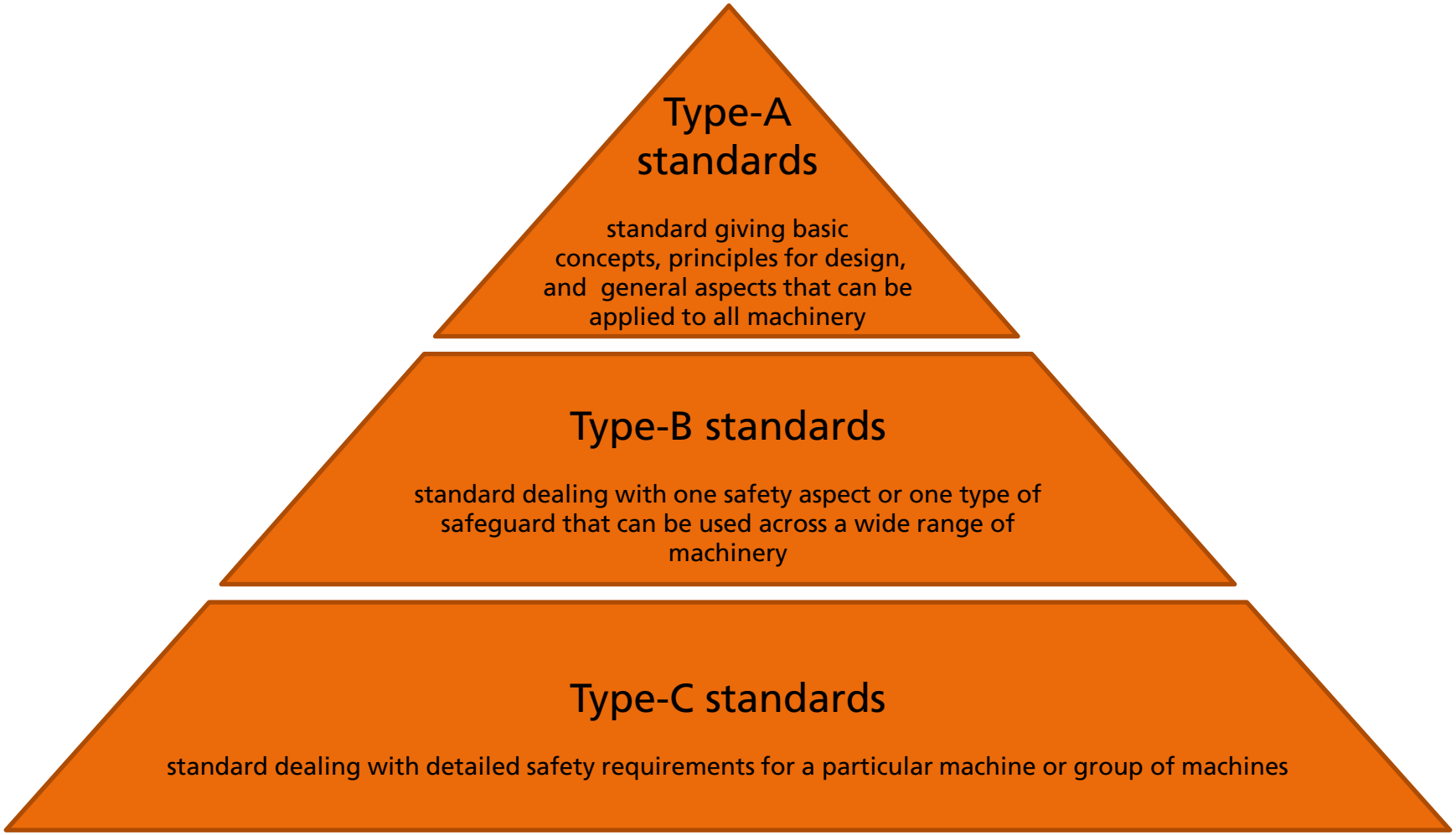
… and their relation to laws

- Governments pass regulations for product safety
- Regulations often refer to national and international standards
  - Compliance with safety standards is mandatory or at least highly encouraged
  - In some cases deviations from standards are accepted, if an equal level of safety is reached
- Example: Safety regulations in the European Union
  - Only products that comply with directives on product safety may be put into circulation on European markets, e.g.
    - 2001/95/EG Product safety
    - 2006/42/EG Machinary directive
    - 93/42/EWG Medical devices

… and their relation to laws

- Example: Safety regulations in the European Union
  - Directives include a list of “harmonized standards”
  - Harmonized standards are not mandatory, but
    - Application of these standards lead to “presumption of conformity” with the directive
    - Shifting of the burden of proof that a product does/does not fulfill requirements
  - Products that comply with all relevant directives may carry the CE mark

Hierarchy of ISO safety standards for machinery



➔More detailed standards shall not contradict general standards

Fraunhofer IPA

Agenda

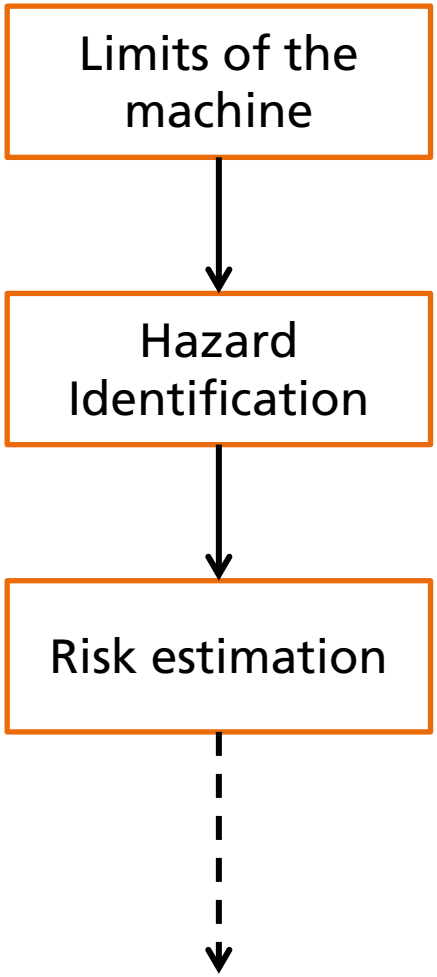
- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Special requirements for industrial robots
  - Special requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

ISO 12100 - Safety of machinery - General principles for design - Risk assessment and risk reduction

Contents:

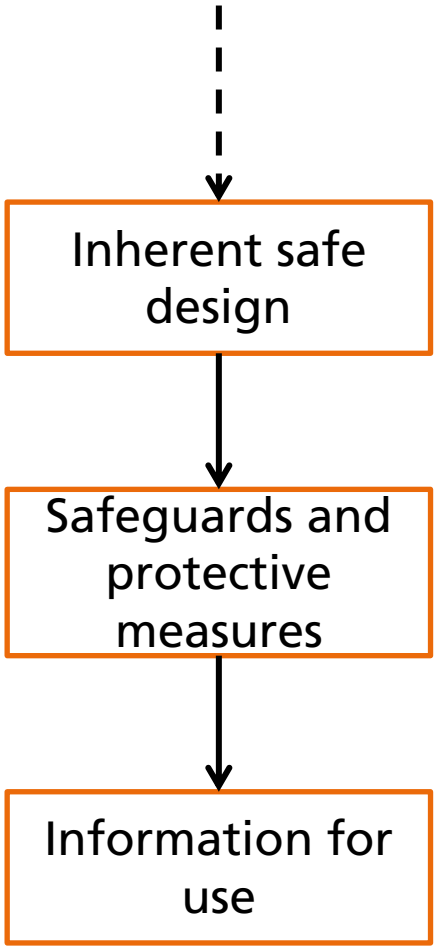
- Foreword
- Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Strategy for risk assessment and risk reduction
- 5 **Risk assessment**
- 6 **Risk reduction**
- 7 Documentation of risk assessment and risk reduction
- Annex A (informative) Schematic representation of a machine
- Annex B (informative) Examples of hazards, hazardous situations and hazardous events
- Annex C (informative) Trilingual lookup and index of specific terms and expressions used in ISO 12100

ISO 12100 – Risk assessment



- Limits of the machine: affected user groups, tasks, environmental conditions, etc.
- Estimation risk connected to a hazard:
  - Severity of the harm
  - Probability of occurrence
- Many different methods for risk estimation possible, e.g. risk graphs, tables, calculation schemes, risk priority number (FMEA)
- Result of risk estimation:
  - List of unacceptable risks
  - Quantitative estimation, how much a risk has to be reduced

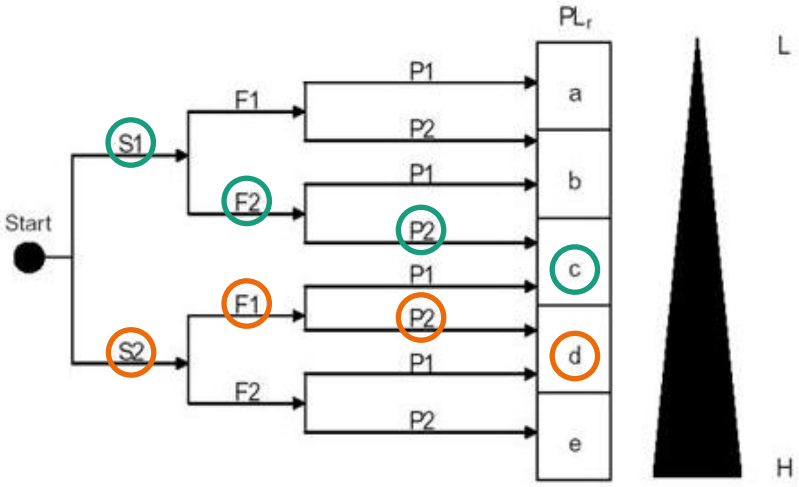
ISO 12100 – Risk reduction



- Inherent safe design: Elimination or reduction of risk by change of mechanical design
  - e.g. low-power-drives to prevent crushing by arm
- Safeguards and protective measures: Reduction of risk by restricting the access to the hazard source
  - e.g. restriction of arm force in control system
- Information for use: User is informed, which risk could not be reduced and how to avoid them
  - e.g. warning signs to keep distance from the arm
- Rules:
  - As far as possible, risks shall be eliminated by inherently safe design.
  - Only if inherent measures are not sufficient, safeguards or protective measures shall be used.
  - If no further risk reduction is possible, residual risks shall be named in the information for use.

ISO 13849 - Safety of machinery - Safety-related parts of control systems - General principles for design

- Applies for protective measures realized as part of the control system, e.g.
  - Safe restriction and surveillance of force exceeded by a robot arm
  - Human presence detection
  - Stability control for bipad robots
- Provides a risk graph to for risk estimation
  - Consideration of severity (S) of the harm, frequency (F) of exposure and possibility (P) to evade lead to a required performance level (PL_r)



S1: Low harm, usually reversible
S2: Severe harm, usually irreversible

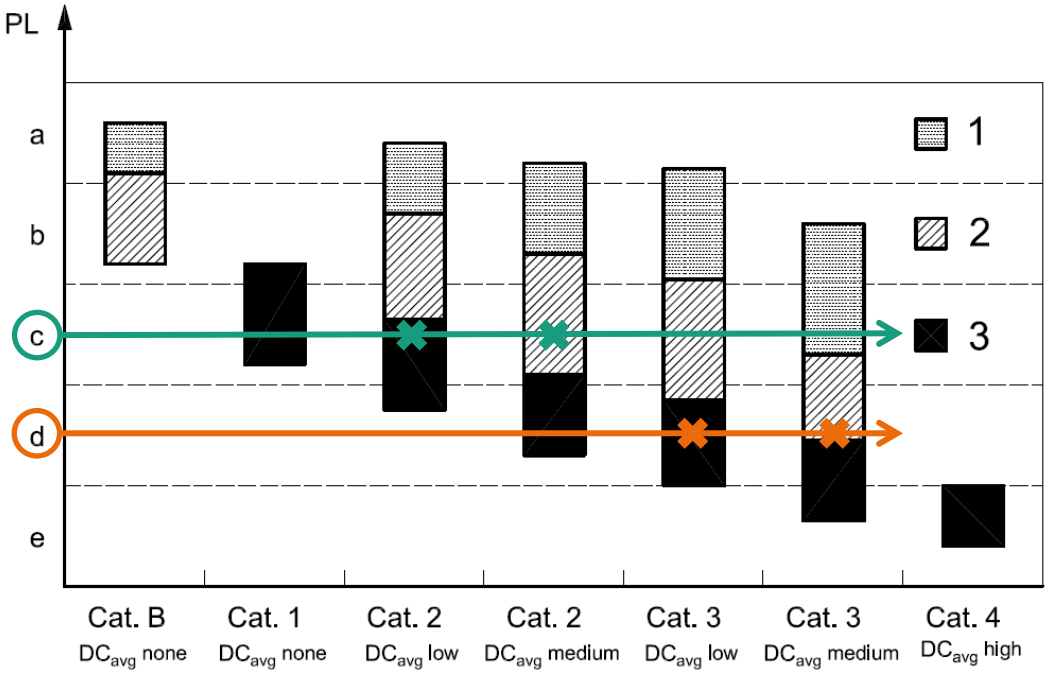
F1: Seldom / low exposure time
F2: Often / high exposure time

P1: Evasion possible under certain conditions
P2: Evasion scarcely possible

Fraunhofer IPA

ISO 13849 - Safety of machinery - Safety-related parts of control systems - General principles for design

- Depending on the required performance level, components of the control systems have to reach a certain safety category, characterized by
  - $MTTF_d$: Meantime to the first dangerous failure
  - DC: diagnostic coverage – percentage of failures detected by a testing system or redundant channel



1: low $MTTF_d$
2: medium $MTTF_d$
3: high $MTTF_d$

Fraunhofer IPA

ISO 13849 - Categories

- Category B, 1: Single channel system
  - Only requirement: Use of well-tested components
  - Single failure might lead to an accident
- Category 2: Single channel system with testing device
  - Cyclic testing of the safety function
  - Dangerous failure is probably detected before it might cause an accident
- Category 3: Two-channel-system
  - Sensors and all parts of the control system exist twice
  - Single failure is always detected and cannot lead to accident
- Category 4: Highly reliable two-channel-system
  - Single failure is always detected and cannot lead to accident
  - Additional protection against accumulation of undetected failures or common-cause-failures

ISO 13849 vs. IEC 62061

- IEC 62061 provides alternate system to estimate risks related to the control system and to specify a required control system performance
- Safety integrity level (SIL) fully compatible to performance level (PL) of ISO 13849

PL	a	b	c	d	e	-
SIL	-	1		2	3	4

- Advantages of IEC 62061
  - Risk graph provides higher granularity
  - Detailed instructions for developing and validating the safety of software
- Disadvantages of IEC 62061
  - Non-electrical control systems (e.g. hydraulics) not covered
  - Application generally more complicated than the application of ISO 13849

Additional standards providing general advice - Examples

Safety distances and approach speeds:

- ISO 13854 - Safety of machinery - Minimum gaps to avoid crushing of parts of the human body
- ISO 13855 - Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body
- ISO 13857 - Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs

Emergency stop:

- ISO 13850 - Safety of machinery - Emergency stop - Principles for design

Extreme temperatures:

- ISO 13732-1/2/3 - Ergonomics of the thermal environment - Methods for the assessment of human responses to contact with surfaces

Agenda

- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Special requirements for industrial robots
  - Special requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

ISO 10218-1/2 - Robots and robotic devices - Safety requirements for industrial robots

Part 1: industrial robot

- Specifies safety requirements for a single industrial robot
  - Mechanical and electrical design of the manipulator
  - Safety related performance of the control system
  - Also: Pendant controls, limiting devices, operational modes, etc.
- Requirement: safety functions shall be realized in PL d and category 3 according to ISO 13849
- First publication in 1992, widely used and adopted to national standardization
- latest revision finished in 2011

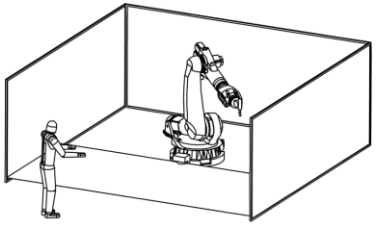
ISO 10218-1/2 - Robots and robotic devices - Safety requirements for industrial robots

Part 2: industrial robot system and integration

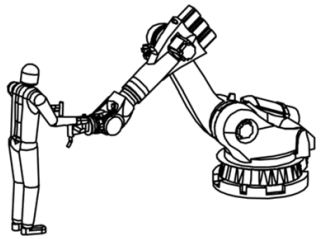
- Published for the first time in 2012
- Specifies safety requirements for systems consisting of robots, tools, workpieces, etc.
  - Rules for integration of robots into a production system
  - Limiting of the robots' workspaces (static and dynamic)
  - Includes tool, workpiece etc. into the risk assessment
- Focus on human-robot-collaboration
  - Different types of collaboration specified
  - Specific safety requirements for different types of collaboration

ISO 10218-2 – Types of human-robot-collaboration

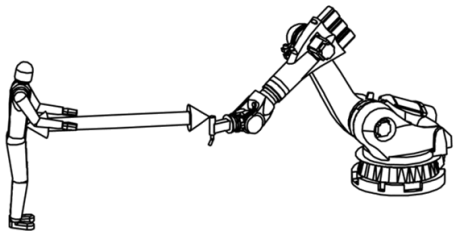
1. Safety-rated monitored stop
   - Robot in normal automatic mode
   - Robot stopps when human enters the workspace and resumes automatically after leaving



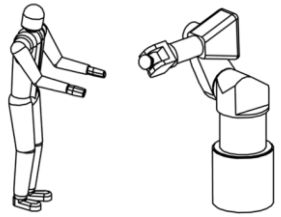
2. Hand guided operation
   - Robot operates at low speed
   - Operation only with enabling switch



3. Speed and separation monitoring
   - Robot operates autonomously at low speed
   - Robot stops when distance to human gets too small

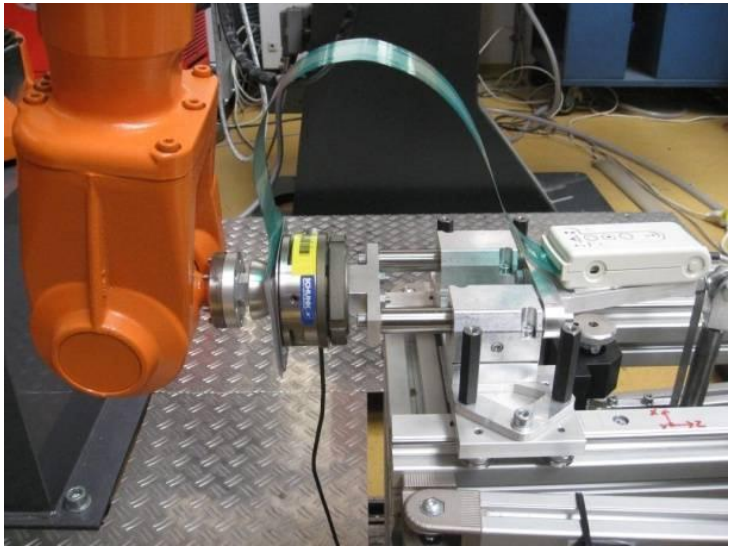


4. Power and force limiting
   - Restriction of force and power of the robot
   - Contact between human and robot allowed



ISO/TS 15066 - Robots and robotic devices - Collaborative robots (draft)

- ISO 10218-1/2: Determination of speed and force limits based on risk assessment
- Problem: Information about effect of impact and force on the human body hardly available
- ISO/TS 15066: Thresholds for impact and force for different parts of the human body based on literature research and practical research of pain tolerances
  - Limits for clamping forces and impact forces
  - Limits for pressure
  - Compression constants
- Instructions for performing impact or clamping tests with testing devices



© Fraunhofer IPA

Agenda

- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Special requirements for industrial robots
  - Special requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

Safety requirements for service robots

- Definition of service robot according to ISO/DIS 8373:

> *"robot that performs useful tasks for humans, society or equipment excluding industrial automation applications"*

- Service robots include a large variety of
  - Robot types and sizes (e.g. humanoids, wheeled robot platforms)
  - Environments (e.g. land-based, swimming, diving, flying, space robots)
  - Tasks (e.g. cleaning, social interaction, inspection, search & rescue)
- Development of a single type-C safety standard for service robots is impossible

© Fraunhofer IPA

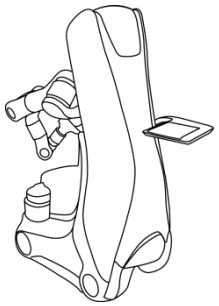

© US Air Force

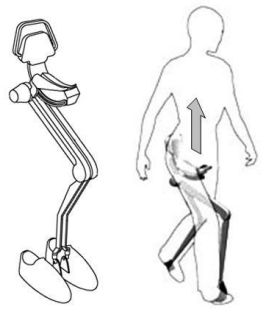

© Aldebaran

Fraunhofer IPA

ISO/DIS 13482 - Robots and robotic devices - Safety requirements for non-industrial robots - Non-medical personal care robot

- Personal care robot → robot in direct interaction with a user, possibly including physical contact
- Further focus on three robot types
  - Mobile servant robot: household assistants etc.
  - Person carrier robot: autonomous wheelchairs, Segways, transport vehicles
  - Physical assistant robot: exoskeletons, orthoses, etc.
- Advice for performing a risk analysis with examples for all robot types
- Measures to reduce risks to an acceptable level (inherent measures, safeguards, documentation of residual risks)
- Definition of safety requirements and minimum control system performance
- First publication in 2013





© ISO 13482 Draft

Fraunhofer IPA

ISO/DIS 13482 – Minimum performance levels for safety-related control system functions

- Minimum levels for control system performance provided for the three robot types
- Where applicable distinction between subtypes with different potential to inflict harm
- Example: Person carrier robot
  1. Single passenger standing on a footboard; robot is small, lightweight, slow (<1,6m/s); robot is semi-autonomous
  2. All other person carrier robots, e.g. large, heavy, fast, with seat/cabin; autonomous transportation of one or more passengers

© ISO 13482 Draft

ISO/DIS 13482 – Minimum performance levels for safety-related control system functions

Safety function	Minimum PL Subtype 1	Minimum PL Subtype 2
Emergency stop	d	d
Protective stop	c	e
Limits to workspace (incl. forbidden area avoidance)	not applicable	e
Safety-related speed control/restriction	c	e
Safety-related force control/restriction	not applicable	not applicable
Hazardous collision avoidance	not applicable	e[2]
Stability (incl. overload protection)	b[1]	d[3]

[1] In case of inherent instability PL c shall be achieved

[2] The control system shall achieve PL e but this may not be achievable for sensing mechanisms. In this case, systematic limits of sensors shall be reduced as low as reasonably practicable.

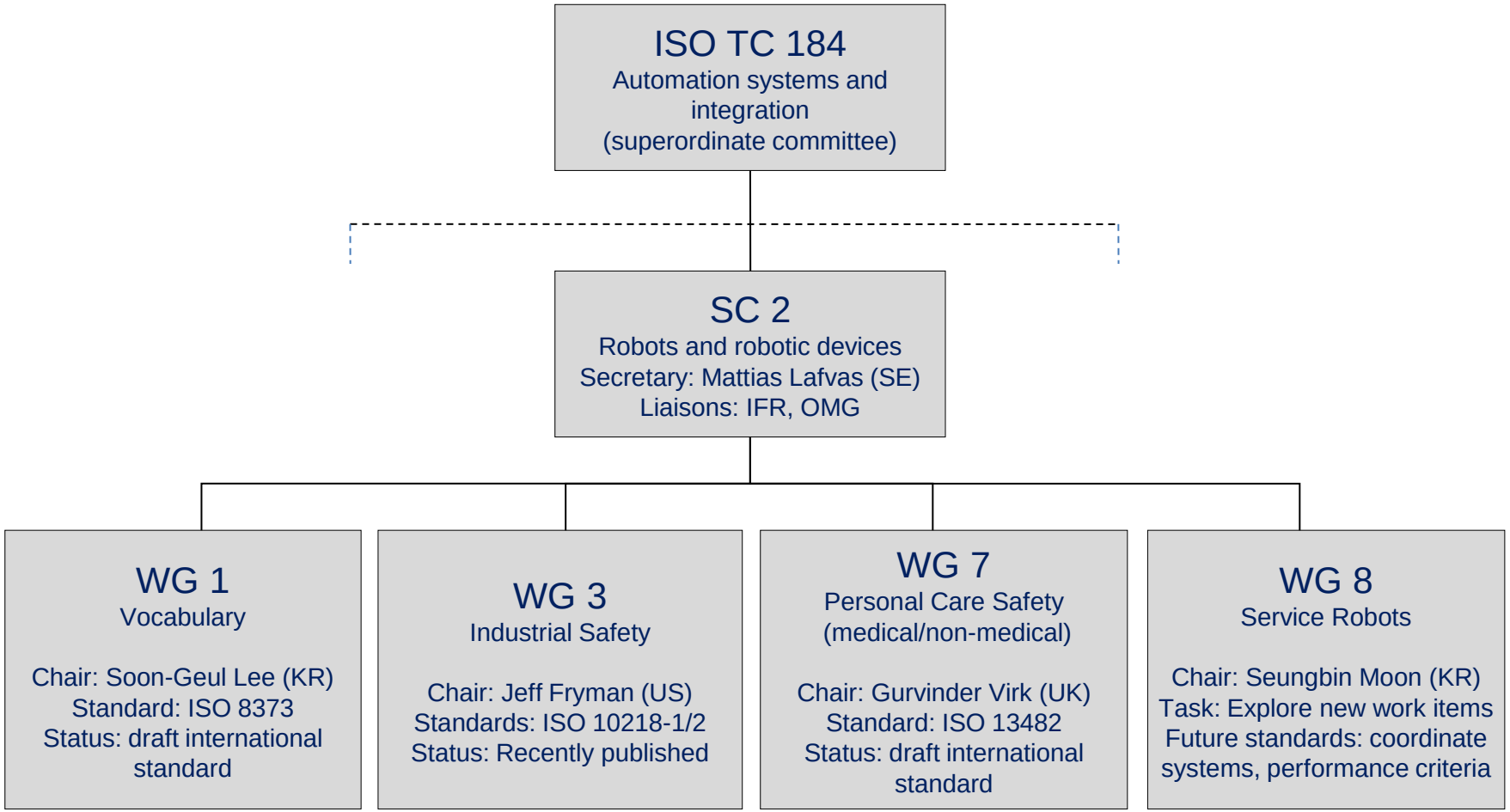
[3] In case of inherent instability PL e shall be achieved.

Fraunhofer IPA

Agenda

- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Special requirements for industrial robots
  - Special requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

Standardization at ISO committee TC 184/SC2



Fraunhofer IPA

Standardization at ISO committee TC 184/SC2

- Working groups meet three times a year at changing locations (US, Europe, Asia)
  - Period of 5 days for service robots (WG1, WG7, WG8)
  - Period of 3 days for industrial robots (WG3)
- Development of the standard though “commenting”
  - Draft documents are distributed to each national standardization organization after a meeting
  - National experts propose changes in the document through comments
  - Processing of all comments in the regular meetings
- Countries currently contributing to the meetings: China, France, Germany, Italy, Japan, Korea, UK, USA
- Additional contributions to WG3: Canada, Sweden, Switzerland

Further development of safety standards

- Safety standards for industrial robots
  - Development of technical specification ISO/TS 15066 on force limits for human-robot-collaboration
  - Inclusion of force limits in ISO 10218-2 in the next revision
- Safety standards for service robots
  - Development of standard ISO 13482 on safety requirements for non-medical personal care robots
  - Development of a safety standard for medical robots in progress
  - Work on standard for performance criteria (including safety related performance) has recently been started, e.g.
    - Breaking distances
    - Stability on certain terrains
    - Person detection capability
    - etc.

Further development of safety standards

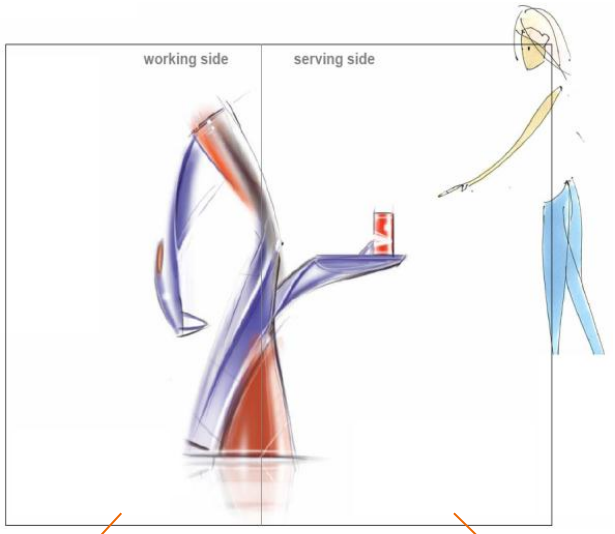
- Possible future safety standards for service robots
  - Development of more detailed standards for
    - mobile servant robots
    - physical assistant robots
    - person carrier robots
    - Additional robot types
  - General standard (probably type-B) for a large group of service robots

- Other standards (non-safety)
  - Terms and definitions (ISO 8373)
  - Coordinate systems (ISO 9787)

Agenda

- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Special requirements for industrial robots
  - Special requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

Inherently safe design – Example: Care-O-bot 3



- Separation of working side and serving side
  - Interaction via tray
  - Arm is folded behind the back during interaction
  - During manipulation the arm is shielded by the robot's body
- Compliant textile cover to reduce the extent of collisions

Inherent safety – Example: Frida (ABB)

- Low-power actuators

  → Robot is too weak to harm a person
- Compliant material to reduce the extent of a collision
- Surface structure without gaps or sharp edges

  → Prevention of clamping inside robot joints and cutting injury

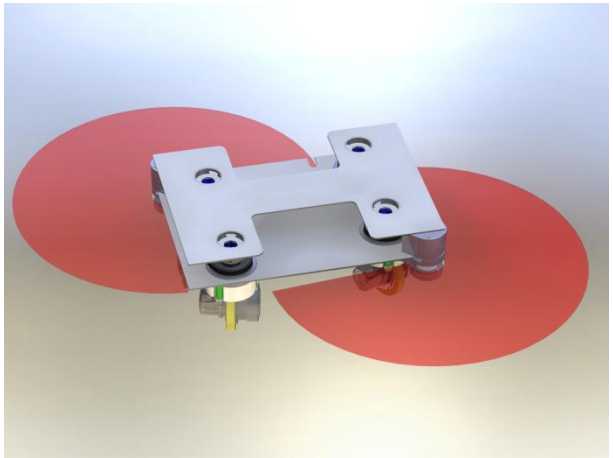
© ABB

Protective measures – collision detection/avoidance

- Pressure-sensitive devices (bumper)
  - Safe contact detection
  - No collision avoidance possible

© SICK

- Light curtains
  - Curtain of laser beams
  - Detection of a human passing the curtain
  - Only for fixed installations (e.g. industrial robot)



- Laserscanner
  - Distance measurement in one plane with rotating laser beam
  - Definition of fields for warning signal/safe stop
  - Mobile application possible

© SICK

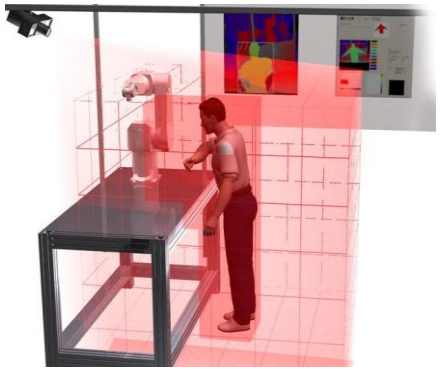
Protective measures – safe camera systems

© SICK


© PILZ

- Detection of reflecor strips in 2D/3D
  - Restricted areas marked with reflector strips
  - Obstacles occlude relflectors
  - Complex protection geometries possible

- Current research topics
  - Use of 3D time-of-flight sensors to detect object and to define 3D collision hulls
  - Collision detection by detecting intersections of collision hulls



© MESA

Fraunhofer IPA

Protective measures – tactile skins for robots

- Whole robot or part of the robot covered with sensitive material
  - Collision detection when the robot touches an obstacle
  - Soft material limits the extent of a collision
- Systems consisting of a small number of large bumper elements already available
- Challenge: Tactile skin with high resolution
  - Large arrays of individual sensors
  - High number of safe inputs to the control system necessary

© MRK

© Roboskin

Agenda

- Introduction: Why robot safety?
- Standards vs. laws
- Safety requirements from standards
  - General requirements
  - Special requirements for industrial robots
  - Special requirements for service robots
  - Further development of standards
- State of the art in safe robot design
- Conclusion

Conclusion

- Robots having the power to severely injure a human must be designed in a safe way
- Standards give advice on how to reduce risks to an acceptable level
  - General standards (type-A, type-B)
    - ISO 12100: Risk assessment and risk reduction by inherently safe design, protective measures and information for use
    - ISO 13849: risk evaluation and required safety-related performance for control systems (performance levels, categories)
    - Standards dealing with safety distances, design of emergency stops etc.
  - Specific standards (type-C) for industrial robots
    - ISO 10218-1: Safe design of industrial robots
    - ISO 10218-2, ISO TS 15066: Safe integration of robots into production systems and safe human-robot-collaboration

Conclusion

- Specific standards (type-C) for service robots
  - Safety standard for all kinds of service robots is not available
  - ISO 13482: Safe design of personal care robots, especially mobile servant robots, physical assistant robots and person carrier robots
- Current and future standards are developed in ISO committee TC184/SC2 in several working groups
- State of the art in safe robot design includes
  - Inherent safe design (low drive power, compliance, etc.)
  - Optical sensors 2D/3D for workspace surveillance
  - Tactile sensors for collision detection
- As research and development of safety sensors evolve, new application will be possible

Thank you for your attention

Fraunhofer IPA