SAFETY REQUIREMENTS AND STANDARDISATION FOR ROBOTS: SOFTWARE DO'S AND DON'TS

Dipl.-Ing. Theo Jacobs, theo.jacobs@ipa.fraunhofer.de

Fraunhofer Institute for Manufacturing Engineering and Automation IPA

Safety as a key factor for bringing innovative robots onto the market

- Current trends in robotics:
    - Collaborative robots and robotic co-workers
    - Modular, reconfigurable systems
    - Increase in complexity of control systems and software
- Challenges for creating and selling new products:
    - Safety and reliability of new robotic applications needs to be guaranteed
    - Legal requirements and safety standards need to be fulfilled

AGENDA

- European Directives on product safety
- Applicable standards for industrial and service robots
- Requirements for "safe software"
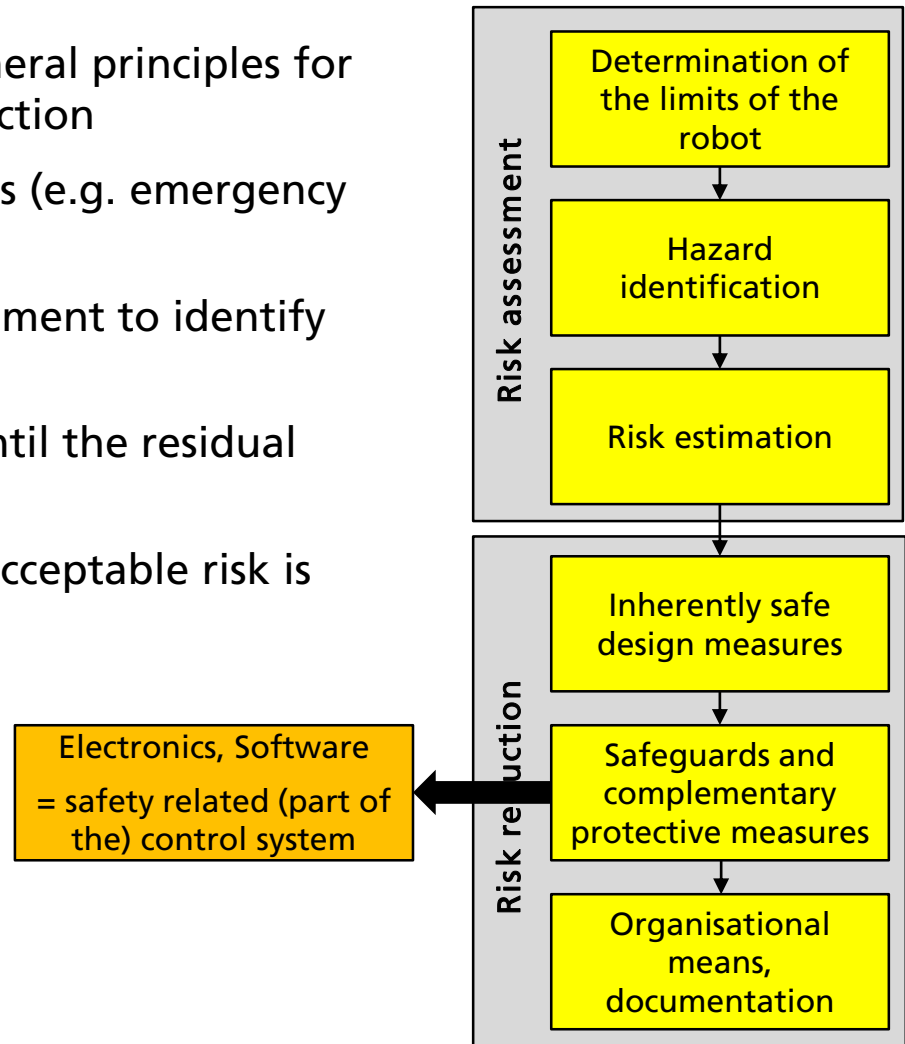- Safety standardisation at ISO

Fraunhofer
IPA

European directives on product safety

- All products put into circulation in the EU (manufactured, sold, imported, operated, etc.), have to fulfill applicable EU directives

  - Example: Machinary Directive (2006/42/EG), Low Voltage Directive (2006/95/EC), EMC-Directive (2004/108/EG)

    - Containing very general requirements for products

    - Conversion into national law (e.g. "Produktsicherheitsgesetz" in Germany)

- Reference to a list of "harmonized standards"

  - Detailed safety requirements

  - Application voluntarily but recommended

  - Presumption of conformity: If all harmonized standards of a directive are fulfilled it is presumed that the directive itself is fulfilled

- If all requirements from EU directives are fulfilled, a CE mark can be applied

Fraunhofer

IPA

Applicable standards: Risk assessment and risk reduction

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

  - General requirements for machines (e.g. emergency stop buttons, start-up, …)

  - Obligation to perform a risk assessment to identify unacceptable risks

  - Reduction of unacceptable risks until the residual risk is acceptable

- Manufacturer has to decide what an acceptable risk is

Risk assessment

- Determination of the limits of the robot
- Hazard identification
- Risk estimation

Risk reduction

- Inherently safe design measures
- Safeguards and complementary protective measures
- Organisational means, documentation

Electronics, Software = safety related (part of the) control system

Fraunhofer IPA

Applicable standards: Control system performance

- ISO 13849-1 – Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design

  - Introduces required performance levels (PL) for safety-related control systems (e.g. velocity and position control, collision avoidance, stability control, etc.)

  - Higher PLs require redundant systems, well-proven components and high diagnostic coverage

- IEC 62061 – Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

  - Definies safety integrity levels (SIL) for safety-related control systems

  - Conversion between PLs and SILs possible

  - Applicable also to software functions

- Use of risk graphs to evaluate severity and likeliness of harm
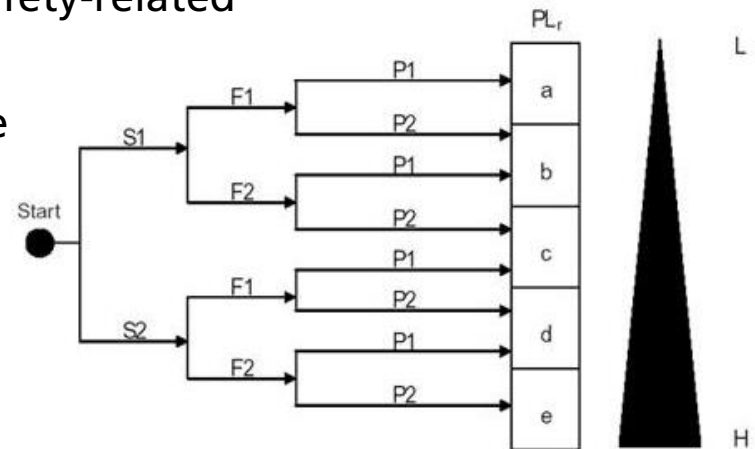
Applicable standards: Industrial robots

- ISO 10218-1 – Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots Requirements for the design of manipulators for industrial environments

    - Examples: mechanical and electrical design, pendant controls, operational modes, etc.

- ISO 10218-2 – Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration

    - Requirements for integrating industrial robots into automation systems

    - Examples: Collaborative modes like monitored stop, hand guiding, velocity or force control

- ISO/TS 15066 – Robots and robotic devices – Collaborative robots

    - Specification of tolerable force and pressure during collisions for different body parts

    - Instructions to measure impact forces and verify limits

Fraunhofer
IPA

Applicable standards: personal care robots

- ISO 13482 – Robots and robotic devices – Safety requirements for personal care robots

- Personal care robot: *"service robot that performs actions contributing directly towards improvement in the quality of life of humans, excluding medical applications."*

  - Examples in the standard: Mobile servant robots, person carrier robots, physical assistant robots

  - Requirements for mechanical and electrical design

  - Requirements for control system design and performance

- New concepts in the area of service robots

  - Shared workspace is the standard case

  - Intended contact between robot and human

  - Risks related to autonomous actions and decisions

© ISO 13482

Fraunhofer

IPA
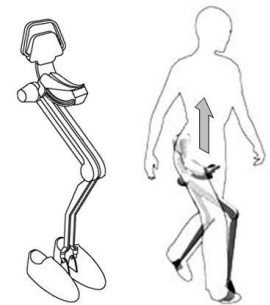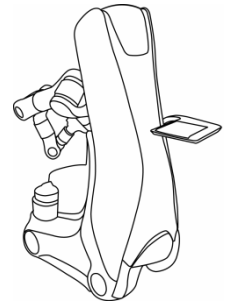
Safe software: Boundaries of the safety-related control system

Levels of the control system

| application software level | 3D position and velocity control, person- and object detection, trajectory planning ,obstacle avoidance, selective muting of safeguards, application of varying protection fields based on situation, safety-related autonomous decisions, … | "sand box" protected by safety-related part |

application software level → 3D position and velocity control, person- and object detection, trajectory planning ,obstacle avoidance, selective muting of safeguards, application of varying protection fields based on situation, safety-related autonomous decisions, …

OS and middleware level →

"sand box" protected by safety-related part

Safety device and PLC level → Light curtains, safety laser scanners, „safe-torque-off", safe program logic, …

safety-related part (state of the art)

Electrical and mechanical level → Relais, limit switches, enabling devices, cutting off drive power, …

Fraunhofer
IPA

Safe software: Extending the boundaries of the safety-related control system

Fraunhofer
IPA
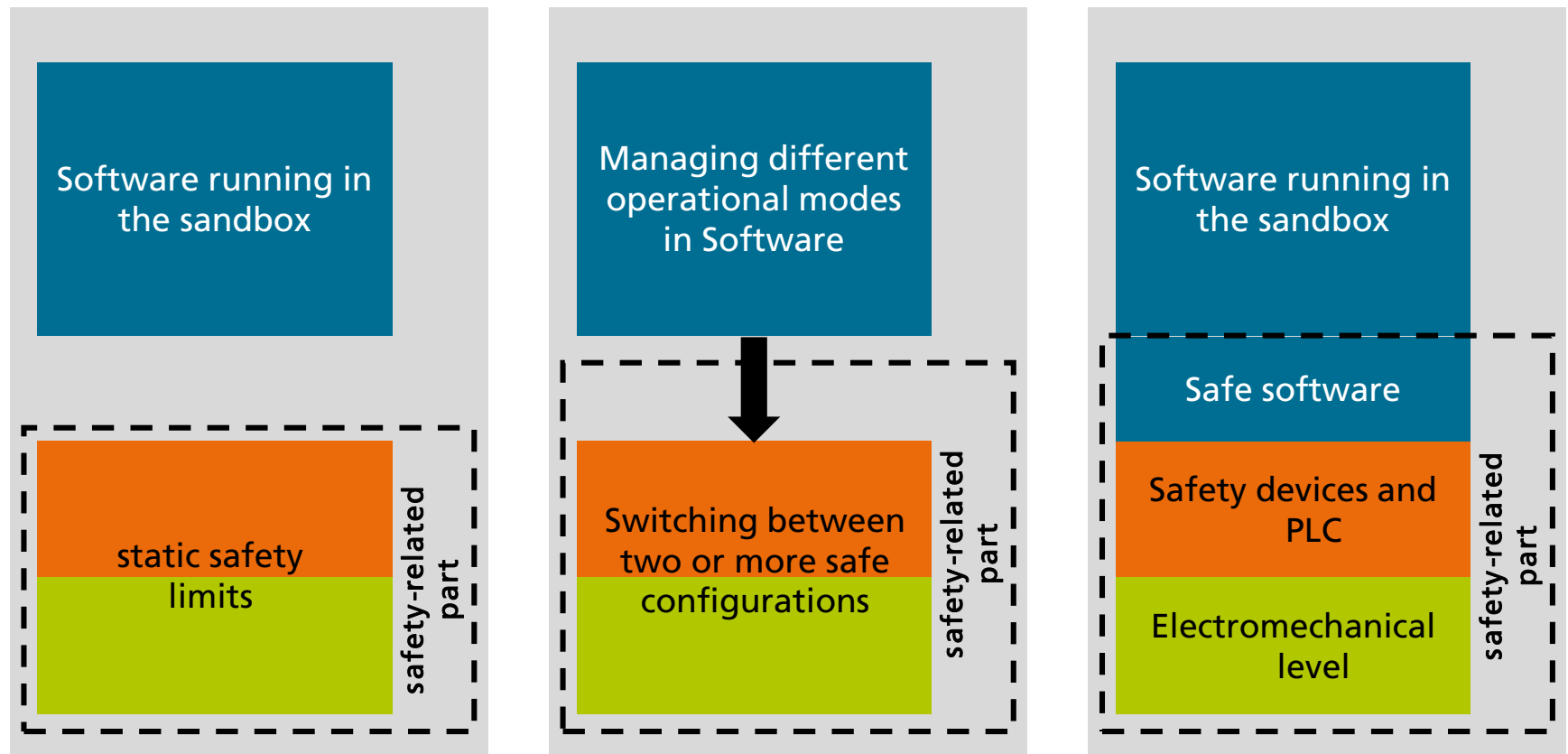
Requirements for designing and writing safe software – Organisational structures

- Applicable standards: IEC 62061 and IEC 61508-3 – Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 3: Software requirements

- Inclusion of software and computer hardware into the risk assessment process; determination of required control system performance (SIL)

  - Performance and reaction times need to be guaranteed

  - Clear separation between safety-related and other parts

- Management of the complete software lifecycle

  - Specification, Development, Validation, Use, Modification

  - Complete documentation of all processes

  - Definition of a detailed validation plan before the development starts

  - Determination of responsible persons for each process step

- Thorough validation at each level of the V-Model and repeated validation of affected parts after any modification

Fraunhofer
IPA

Requirements for designing and writing safe software – Code development

- Implementation of integrity checks at runtime-level

    - Cyclic self-tests of software and hardware integrity

    - For higher SILs: Redundant and diverse data processing

- Recommendation of methods and restrictions for the software development and validation process, e.g.

    - Use of well-established programming languages, where possible with a certified compiler

    - Avoiding error-prone code features such as dynamic objects, pointers, automatic type-conversions, etc.

    - Use of style-guidelines and structured programming methodologies

    - Architectures where process software and integrity checks run independent from each other

Fraunhofer
IPA

Possible conflicts between open source software and requirements for safe software

Requirement/Recommendation		Reality in OSS development
Risk assessment considers a certain application with defined boundary conditions	⇄	Re-use of code in various software projects with different application and conditions
Creation of validated software versions, Protection against uncontrolled modification	⇄	Free alteration, recombination and forking, No control for the developer who uses his software
Management of the complete software lifecycle with clear responsibilities and full documentation	⇄	Loosely connected development teams, limited trust between developers, varying quality of documentation
Legal responsibility of a single entity (manufacturing company), contracts with suppliers	⇄	End user is responsible for the complete software, no legally binding agreements with developers

Conclusion: Possibly only works for

- Self-contained modules maintained by a small group of programmers
- Verified software versions with change-on-your-own-risk policies

Fraunhofer
IPA

ISO Standardisation committee TC 299

```
                        ┌─────────────────────────────┐
                        │          TC 299             │
                        │                             │
                        │         Robotics            │
                        │                             │
                        │ Secretary: Katarina         │
                        │        Widström (SE)        │
                        └─────────────────────────────┘
```

Working Group 1	Working Group 2	Working Group 3	Working Group 4	Joint Working Group 5	Working Group 6
Vocabulary and characteristics	**Personal care robot safety**	**Industrial Safety**	**Service Robots**	**Medical robot safety**	**Modularity for service robots**
Chair: Soon-Geul Lee (KR)	Chair: Gurvinder Virk (UK)	Chair: Roberta Nelson Shea (US)	Chair: Seungbin Moon (KR)	Chair: Gurvinder Virk (UK)	Chair: Gurvinder Virk (UK)
Standards:	**Standards:**	**Standards:**	**Standards:**	**Standards:**	**Standard:**
• ISO 8373 (Terms and definitions, published) • ISO 9787 (Coordinate systems, published) • ISO/DIS 19649 (Vocabulary for mobile robots)	• ISO 13482 (Safety for personal care robots, published) • ISO/CD TR 23482-1 (Verification & validation methods for ISO 13482) • ISO/CD TR 23482-2 (Application guide for ISO 13482)	• ISO 10218-1/2 (Safety for industrial robots, published) • ISO/TS15066 (Safety for collaborative industrial robots, published) • Technical reports on manual load/unload stations, end effectors (new work items)	• ISO 18646-1 (Loco-motion performance, published) • ISO/WD 18646-2 (Navigation performance) • Tasks: Contact with liaisons (IEC, OMG); Explore need for additional standards	• IEC/DTR 60601-4-1 (Report on autonomy) • IEC/NP 80601-2-77 (Safety for surgical robots) • IEC/NP 80601-2-78 (Safety for rehabilitation robots) • Joint working group with IEC/SC 62A and IEC/SC 62 D	• Modularity for service robots (preparation of new work item)

Fraunhofer IPA

Standard development in ISO TC 299

- Working groups meet three times a year at changing locations (US, Europe, Asia)
- Instruments for developing a standard
    - Commenting – national experts propose changes in the document through comments
    - Homework – a small group of experts (e.g. one country) introduces new text
    - Balloting – official voting before a draft enters the next development step
- Countries currently contributing to the meetings: Canada, China, France, Germany, Japan, South Korea, Netherlands, Sweden, Switzerland, UK, USA
- Funding for travel costs for interested experts provided by FP7-Project RockEU 2
    - Goal: Ensure participation of European experts in sufficient strength
    - Reimbursement of travel costs and accommodation during a meeting
- Next meetings:
    - All WGs: November 7th to 18th in Orlando, Florida, United States
    - WG 1, 2, 4, 5, 6: February 6th to 17th 2017 in Daegu, South Korea

Fraunhofer

IPA

Conclusion

- Safety regulation for robots

  - Mandatory European directives on product safety

  - Extended by various harmonized standards

- Safe software:

  - Currently often excluded from safety-related part of the control system

  - IEC 61508-family specifies requirements for management, development and validation of code

  - Possible conflicts between safety requirements an principles of open source software

- Standardisation as a living process:

  - Continuously development and alteration of robot-related standards

  - Possibility to become a part of the standardisation process

Fraunhofer

IPA