Elective in Robotics/Control Problems in Robotics

Physical Human-Robot Interaction

Dependability and Safety Standards

Prof. Alessandro De Luca

DIPARTIMENTO DI INGEGNERIA INFORMATICA
AUTOMATICA E GESTIONALE ANTONIO RUBERTI

SAPIENZA
UNIVERSITÀ DI ROMA

Safety in pHRI

- management of risk for humans working near robots involve in general very broad considerations, including
  - potential electrical and pressurized fluid hazards
  - pinching hands or feet
  - dropping parts ...
- most dangerous risk specific to robotics is probably when, in an unspecified instant during a robot movement, a collision occurs or an unwanted force is exerted between robot and human
- even just in this situation, safety of pHRI involves several aspects and depends on many factors
  - software dependability
  - possible mechanical failures
  - human errors in interfacing with the robot ...

Safety in pHRI

traditional approaches have addressed safety by

- modifying controllers for rigid robot manipulators (stiffness, impedance control, force control)
- adding sensors (force, contact, proximity, vision, …)

there are however intrinsic limitations to the extent by which a controller may alter the behavior of a robot

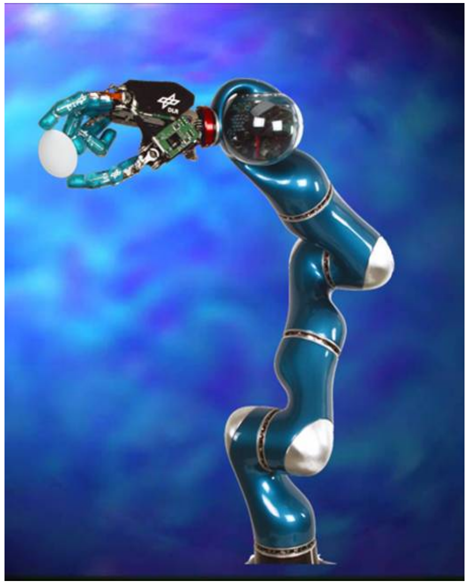
- it is critical when the mechanical bandwidth (dictated by robot inertia and friction) is not matched to the task [Townsend 1988]
- or, stated differently, …

making a rigid/heavy robot behave gently and safely is almost hopeless, when realistic conditions are taken into account

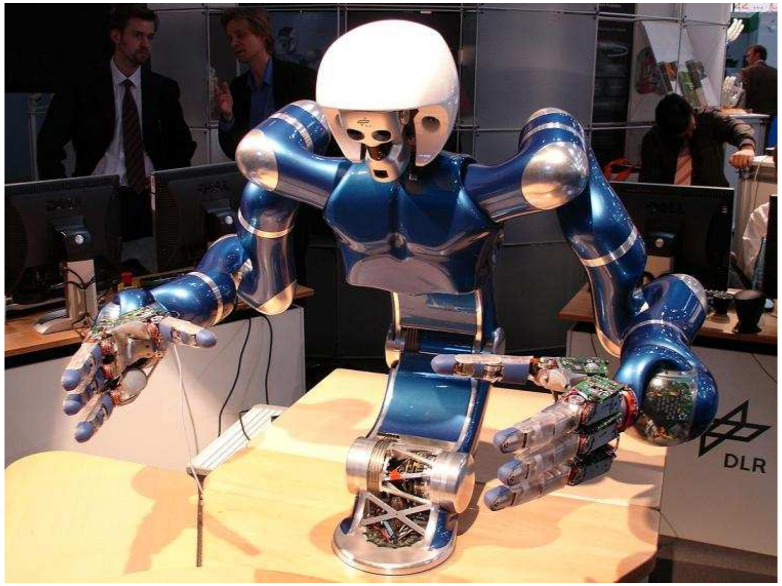
Lightweight manipulators

WAM cable-driven robot
(Whole Arm Manipulation)
by Barrett Technology
[Salisbury, 1988]

DLR LWR generation
[Hirzinger, 2001]



LWR-III with payload equal to its own weight (13.5 kg)



Justin: 2 LWR arms with torso

technological innovations in actuators, sensors, and structural design

Compliant manipulators

- motors contribute for the most part of the effective inertia in conventional geared drives of robots
- compliant transmissions may negatively affect performance, in terms of slow response, larger oscillations and longer settling time
- not a problem for some robotic applications, e.g., entertainment
- when performance matters, co-design techniques of mechanics and control for “soft” robots that are passively compliant, yet fast, strong, and accurate enough

intentionally introduce mechanical compliance in the robot design

Dependability in pHRI

dependability is an integrated concept that encompasses various different attributes [Avizienis et al., 2004]

- safety needs to be ensured both during nominal operation of the robot, as well in the presence of faults
- survivability enforces a robot operation which is safe for the human (completion of a programmed task may even be abandoned)
- availability and reliability a robot must be always ready to carry out its intended tasks, and able to complete them successfully
- integrity relates to the robot physical and logical resources, and requires suitable protection mechanisms against malicious events
- maintainability concerns both physical and logical resources of the robot, which should be easy to repair and to upgrade
  - there is indeed a trade-off between reliability/maintainability on one side, and safety on the other

Fault types

- physical (or internal) faults including both natural hardware faults and physical effects due to the environment
- interaction (or external) faults including issues related to human-to-robot collaboration and robot-to-robot cooperation, robustness issues with respect to operation in an open and unstructured environment
- development faults which may be introduced, usually accidentally, during the design or implementation
- possible faults in the robotic system need to be handled thoroughly, from prevention to diagnosis and prediction

Handling of faults

- fault prevention to prevent the occurrence or introduction of faults (by design)
- fault removal to reduce the number and severity of faults
- fault detection and isolation to recognize the occurrence of a fault and characterizing its location/type
- fault tolerance to avoid service interruption (or large degradation) in the presence of faults
- fault forecasting to estimate the present number, the future incidence, and the likely consequences of faults

Fault handling and dependability

- to preserve the safety of humans interacting with robots during the execution of interaction tasks, fault handling and fault tolerant control have to be considered as fundamental functionalities
- dependability is related to the ability of the system to cope with failures
- to ensure acceptable levels of robot dependability attributes in pHRI, it is useful to explicitly define the types of faults
- achieving dependability requires the application of a sequence of activities for dealing with faults
- fault prevention and removal are collectively referred to as fault avoidance
- a complete fault diagnosis requires fault detection and isolation, and identification of the fault evolution over time
- developing a system with fault tolerance and forecasting is collectively referred as fault acceptance
- incorporation of redundancy in HW and SW plays an important role here

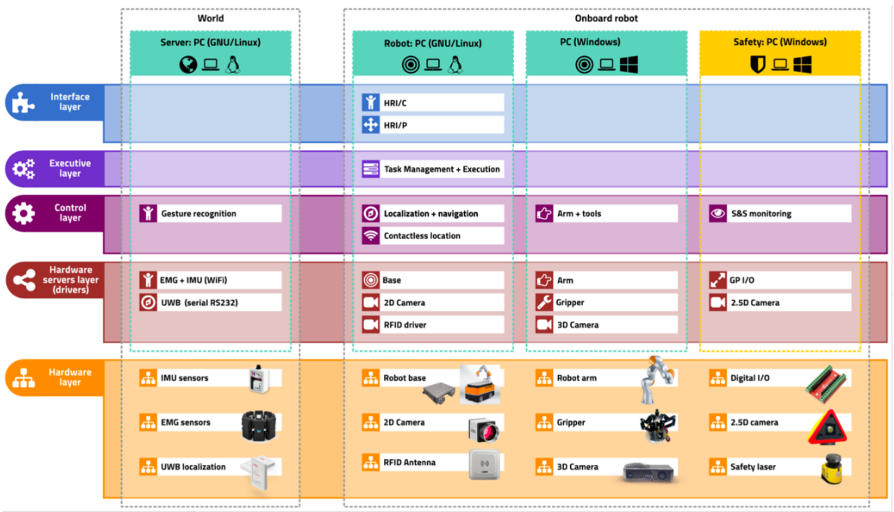
Sensors and dependability

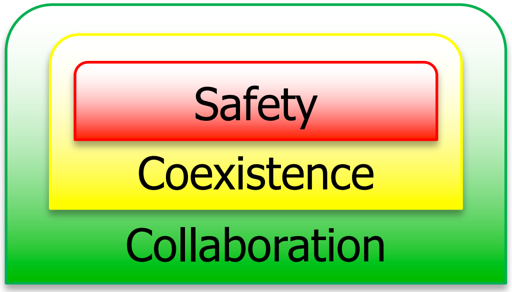
- the selection, arrangement, and number of sensors (as well as their single reliability) contribute to the measure of dependability
- the construction of a good model of humans interacting with the robot is one of the main purposes of a sensory system for pHRI
- sensors must be robust to changing of environmental conditions like lighting, dust, and other sources of uncertainty
- fusion of the information coming from multiple sensors may help in providing a coherent and reliable description of the world surrounding the robot
- inference and learning systems may organize sensory sources and data, taking into account the information about the specific phases of a physical/cognitive interaction task

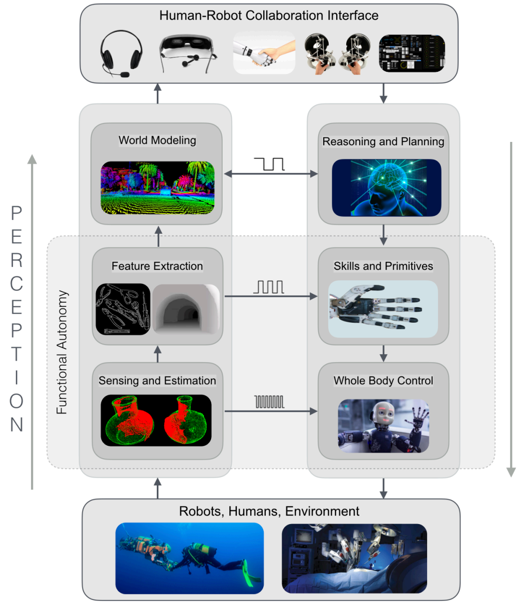
Control architecture and dependability

dependability of the robot control software for pHRI calls for a modular and hierarchical architecture

- advantageous for testing the single components
- allows a simpler isolation of possible faults
- achieves operating robustness
  - in terms of availability, reliability, and maintainability







Control architecture and dependability

- programmability the robot should be able to achieve multiple tasks described at an abstract level
  - its basic functionalities should therefore be easily combined according to the task to be executed
- autonomy and adaptability the robot should be able to carry out its actions and to refine or modify the task and its own behavior according to the current goal and execution context as it perceives it
- reactivity the robot has to take into account events with time bounds that are compatible with the correct and efficient achievement of its goals (including its own safety) and the dynamics of the environment
- consistent behavior the reaction of the robot to events must be guided by the objectives of its task
- robustness the control architecture should be able to cope with failures, exploiting also redundancy of the processing functions and subsystems
  - robustness will require the control to be decentralized to some extent

Standards

- standards are the most important means of addressing and solving safety problems in the workplace
- research work on pHRI has been influenced by the available standards, and has had (and will have) an impact on their evolution
- safety standards for industrial robotics have undergone in the last two decades a rather revolutionary change
- the previous situation included well established national standards (e.g., ANSI-RIA R15.06-1986 in the USA, CSA Z434:2003 in Canada, DIN ICS53 in Germany, etc.) that were collected and harmonized in the first release of the (two-part) ISO 10218 standard in 2006
- previous standards were imposing human-robot segregation as the cornerstone of safety in the workplace

Most salient changes in standards

- control reliability
  - former standards relied upon hardwired electro-magnetic components
  - new ones allows safety-related control circuitry to use state-of-the-art electronic, programmable, network-based technology (and wireless)
- safeguarding and clearance
  - minor changes in clearance distances (about 0.5 meters)
  - a major step towards fully removing the safeguarding requirement, provided that appropriate new/enhanced capabilities and features are possessed by the robot control system itself
- new modes of operation requirements developed for
  - synchronized robot control
  - mobile manipulators mounted on Automated Guided Vehicles (AGV)
  - assisting robots that work in collaborative workspaces with operators

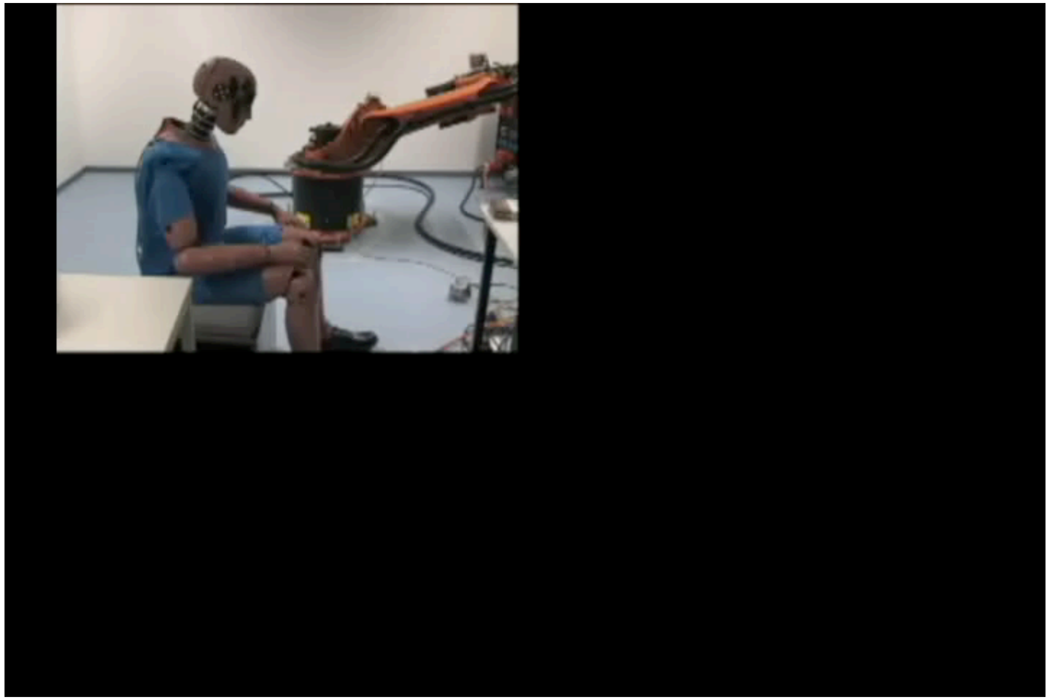
Most salient changes in standards

in addition, few items coming from standardization of IAD systems

- risk assessments in place of fixed rules to identify and mitigate risks in proportion to their seriousness and probability
- safety critical software software and firmware-based controllers should lead, under any single component failure, to the shutdown of the system in a safe state
  - achieved by microprocessor redundancy, diversity, and self-checking
- dynamic limits physical limitations of users are considered by requiring that operators can "outrun, overpower, or turn off" IADs
- emergency stops reliance on "red mushroom" button felt as hazard
  - application-specific external devices initiate context-based safety stops
- (hu)man-machine interface IADs (& robots) should operate in few different modes (hands-off, hands-on-controls, hands-on-payload, etc) that are well communicated to/commanded by the operator

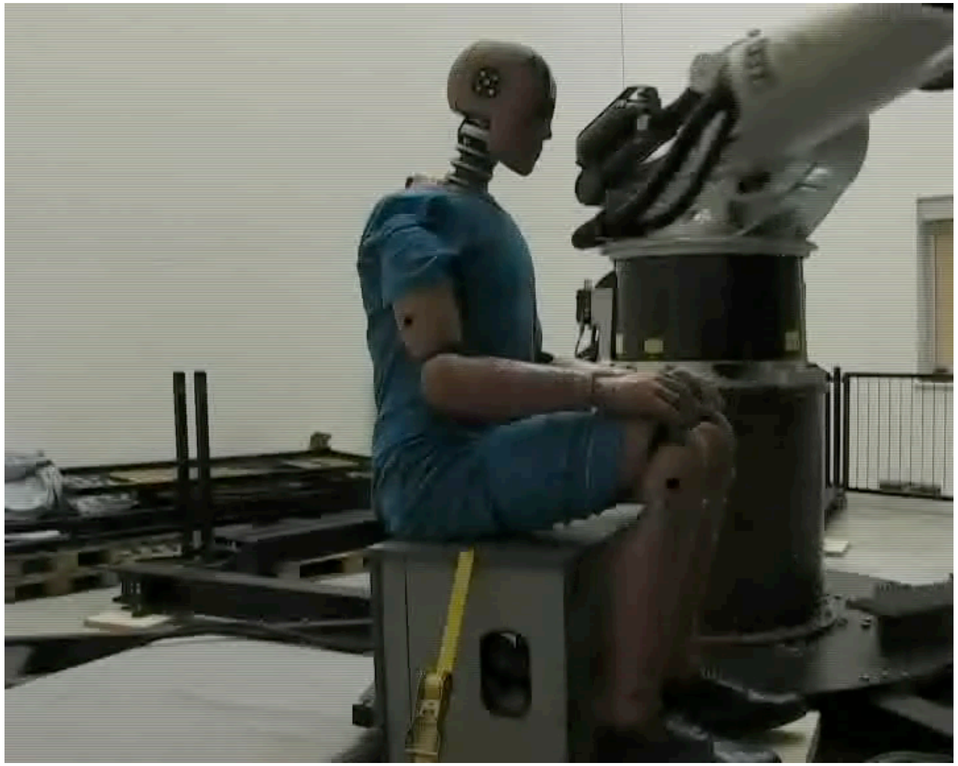
Handbook of Injury

crash-tests: industrial robots-dummy



video

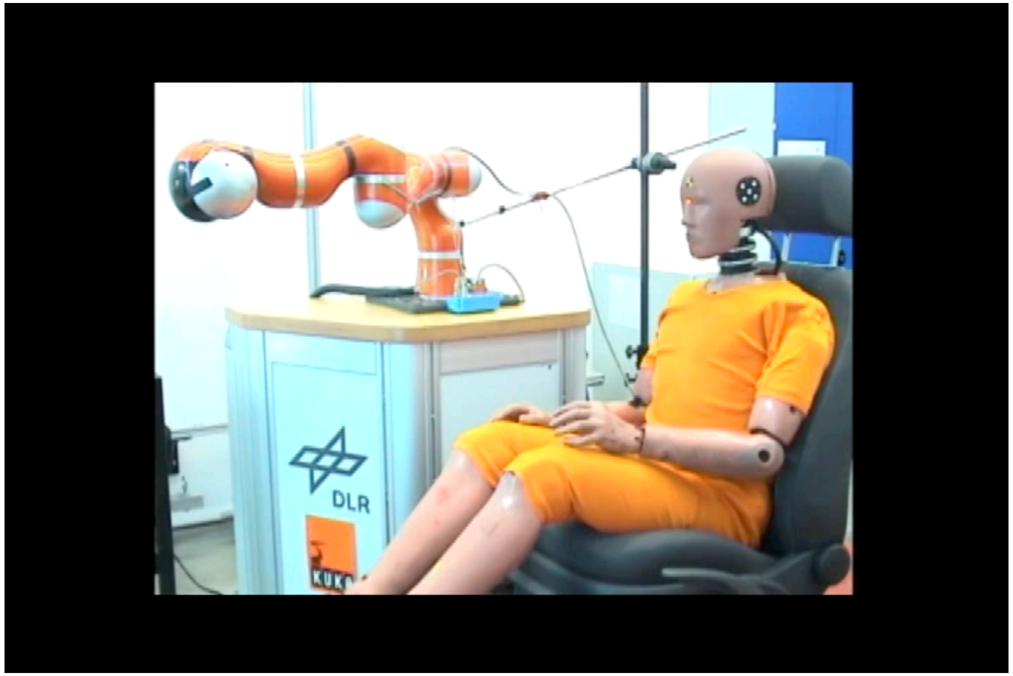
crash-tests: phases and models
in a collision sequence with dummy



video

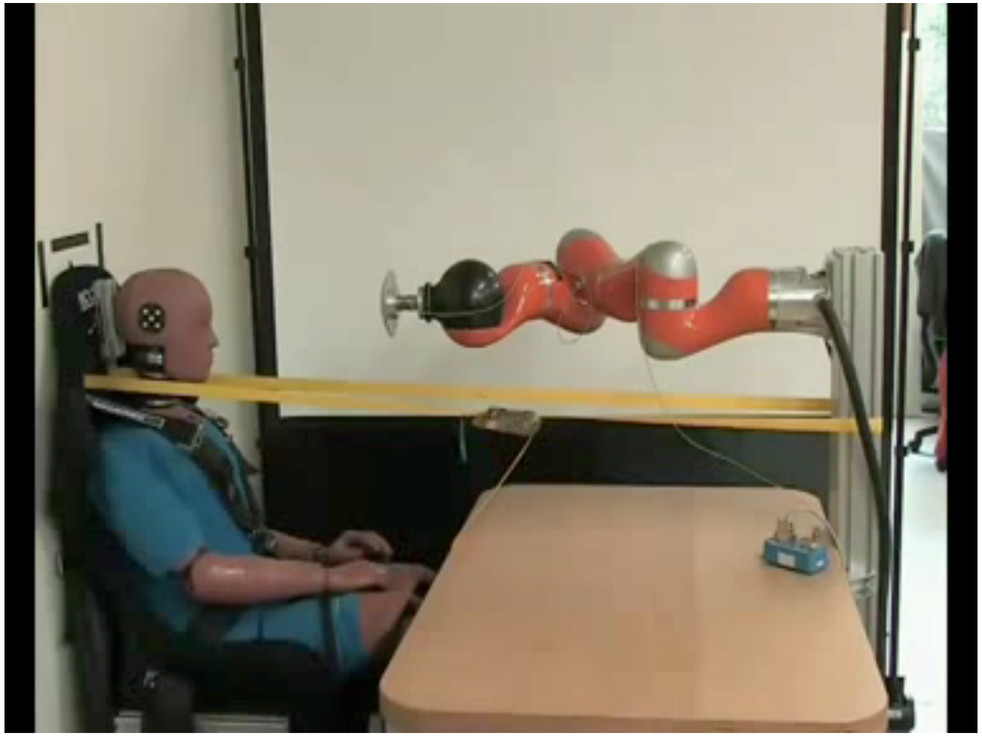
Handbook of Injury

crash-tests: KUKA LWR-dummy
with collision detection/reaction



video

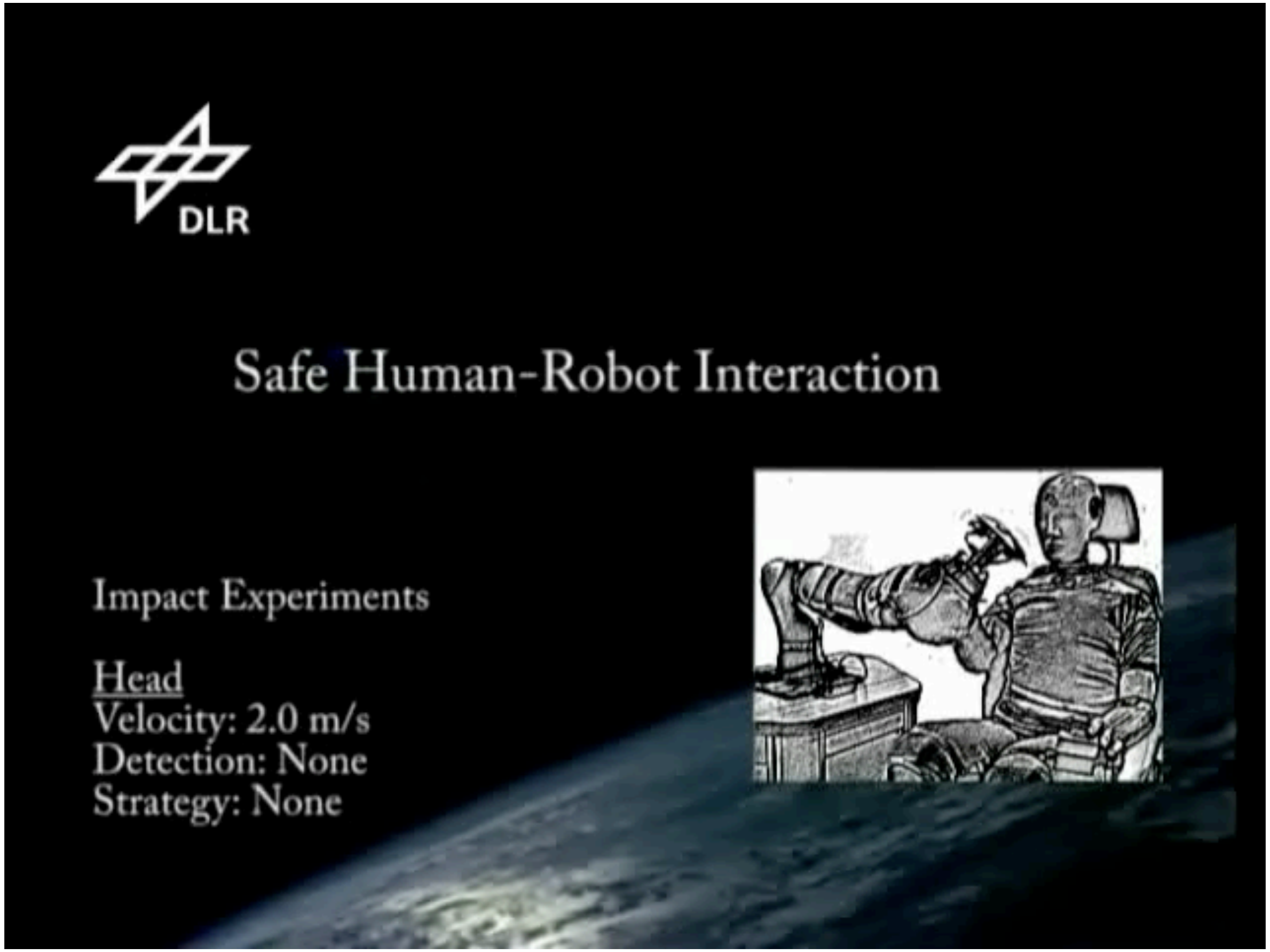
crash-tests: singularity clamping
without and with collision detection



video

Handbook of Injury

comparative assessment of KUKA LWR-dummy impacts
with and without collision detection/reaction

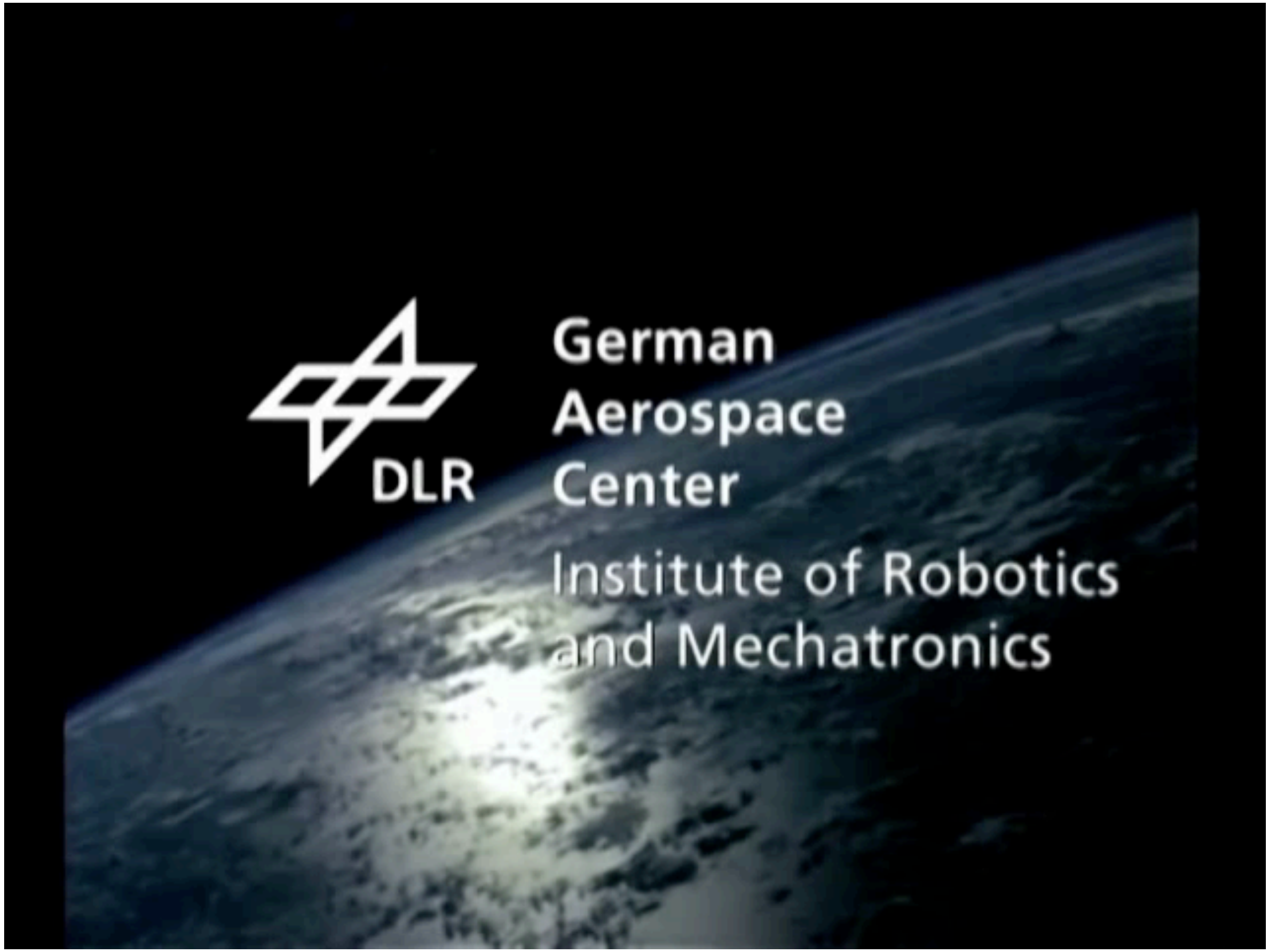


DLR
KUKA
ADAC

video

Handbook of Injury

evaluation of HIC criterion in blunt and unconstrained impacts

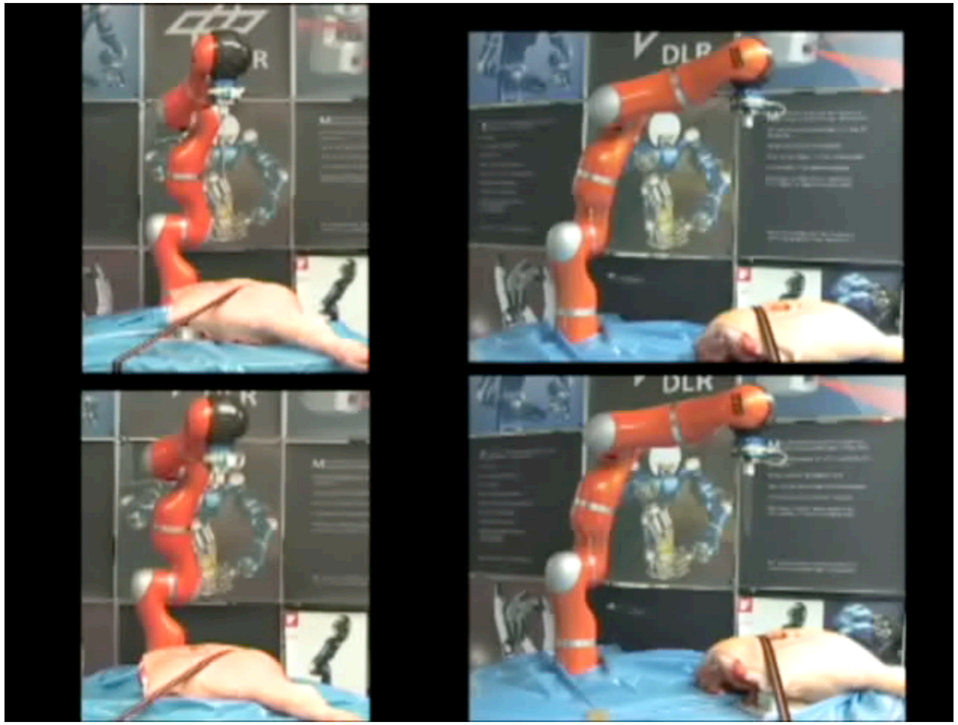


video

http://handbookofrobotics.org/view-chapter/69/videodetails/608

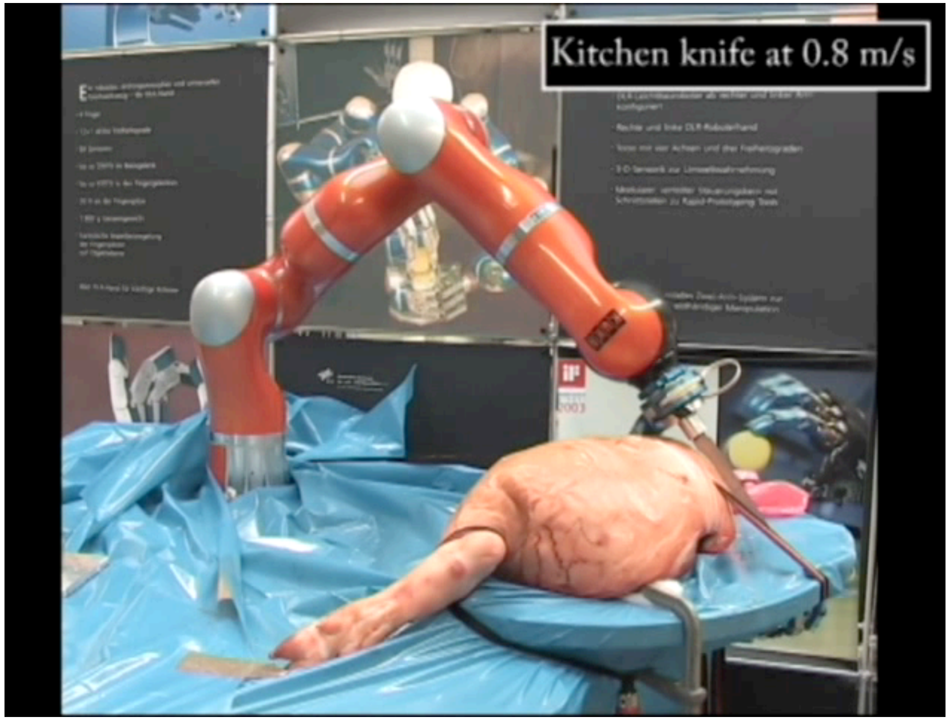
Handbook of Injury

stabbing tests



video

cutting tests



video

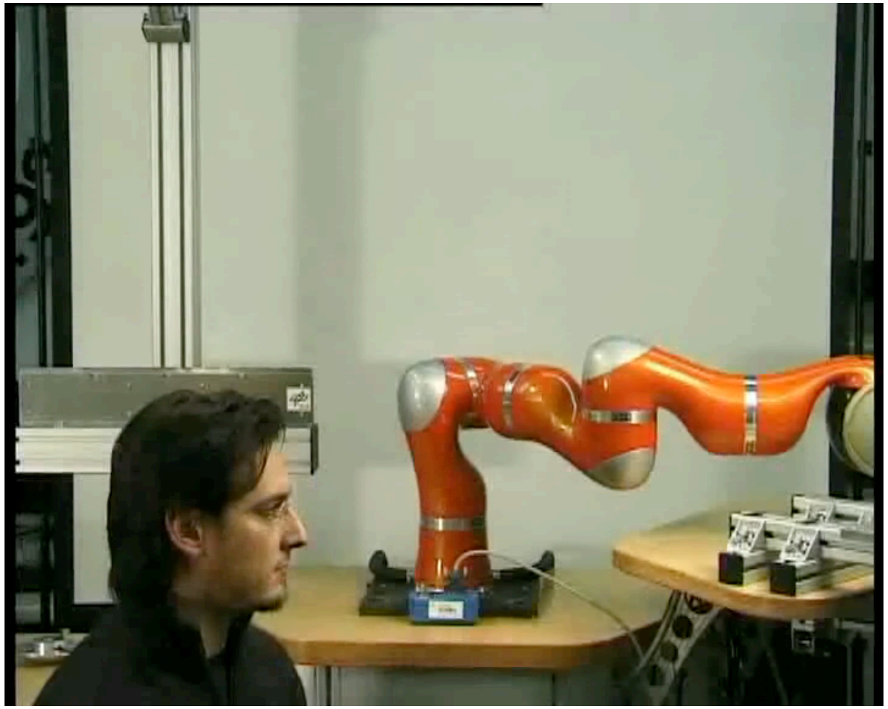
constrained impacts with sharp tools

Collision detection and reaction

chest impact: human

video

head impact: human

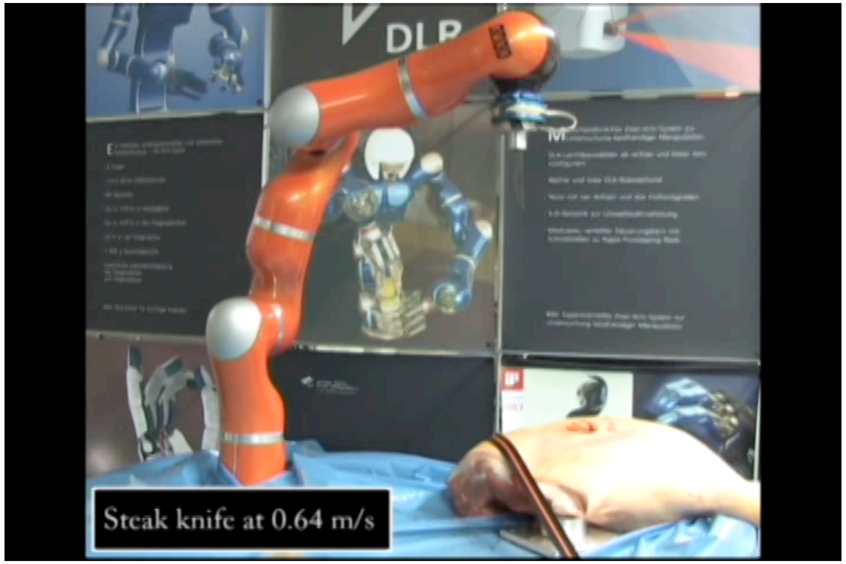


video

the method works for blunt and unconstrained impacts …

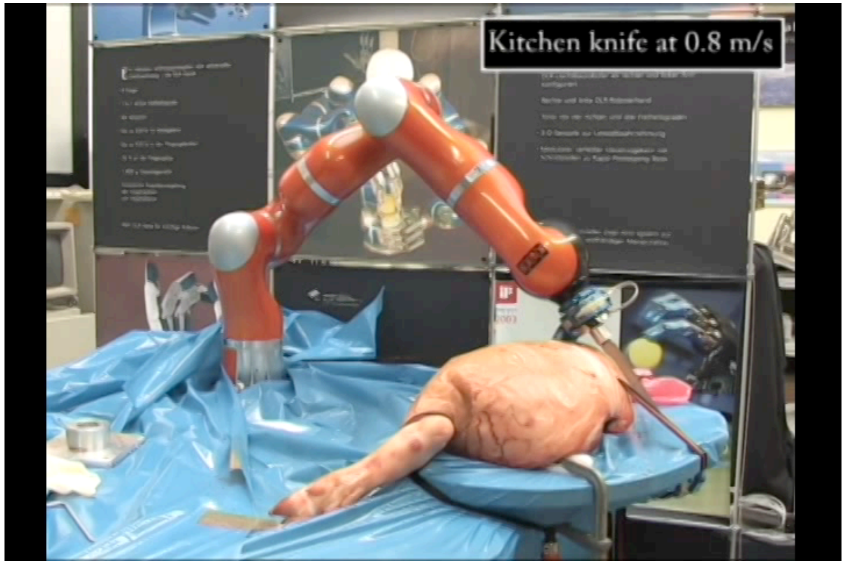
Collision detection and reaction

stabbing with collision detection



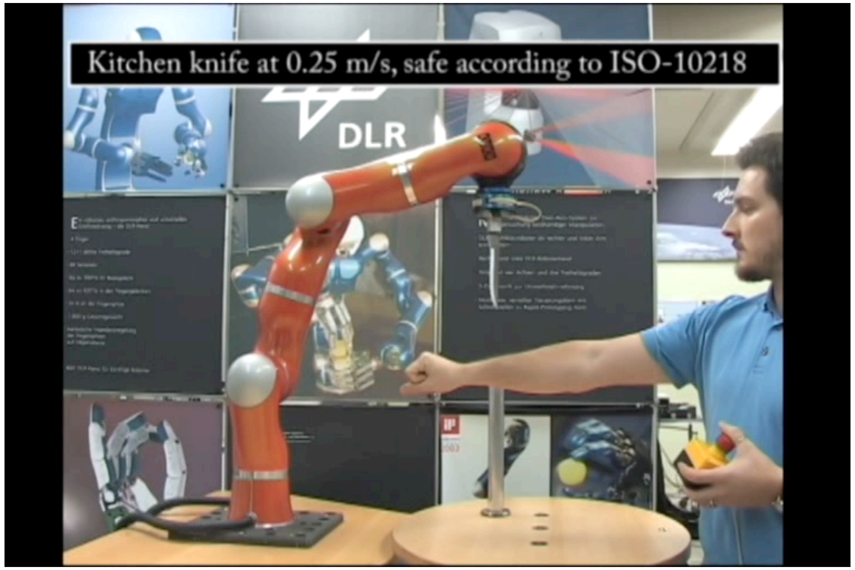
video

cutting with collision detection



video

stabbing a human
with collision detection



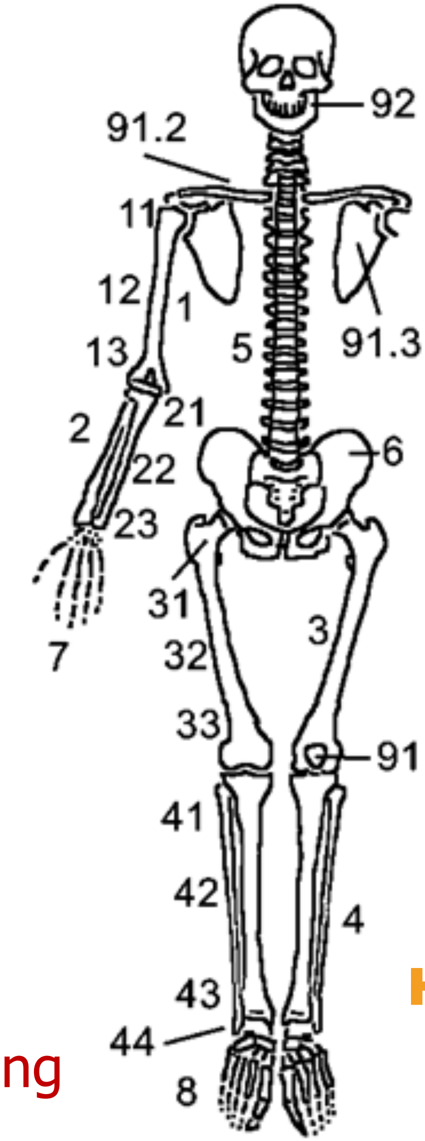
video

Handbook of Injury

AO-classification
Arbeitsgemeinschaft für **O**steosynthesefragen

Motivation
No soft-tissue injury classification exists

Proposal
AO-classification of concomitant injuries in traumatology with description of
- skin damage (I)
- muscle- and tendon-injury (MT)
- nerve- and vessel-injury (NV)



skeletal coding

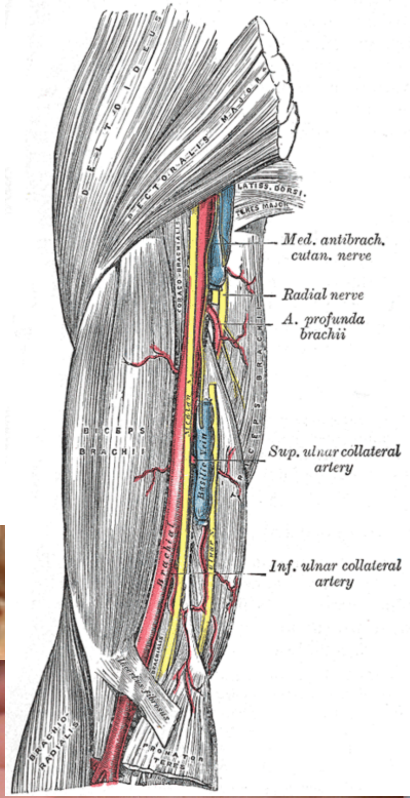
Adjusted AO-classification

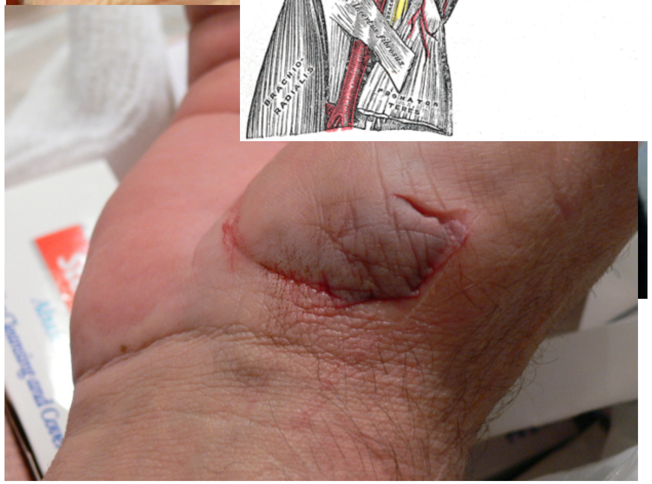
skin damage in a closed fracture
- IC1: NO skin injury
- IC2: contusion without skin opening ← threshold: key impact
- IC3: circumscribed décollement (avulsion)
- IC4: extensive, closed décollement (avulsion)
- ~~IC5: necrosis by deep contusion~~

open skin injury
- ~~IO1: skin puncture from inside to outside~~
- IO2: skin puncture from outside <5cm with contused margins
- IO3: skin lesion >5cm, circumscribed decollement with marginal contusions
- IO4: skin loss, deep contusion, abrasions
- IO5: extensive, open decollement

muscle and tendon injury
- MT1: NO injury
- MT2: circumscribed muscle injury (limited to a muscle group)
- MT3: extensive muscle involvement (2 or more muscle groups)
- ~~MT4: avulsion or loss of a whole muscle group, severed tendon~~
- ~~MT5: compartment syndrome, crush syndrome~~

neurovascular injuries
- NV1: NO injury
- NV2: isolated nerve lesion
- NV3: circumscribed vascular injury
- NV4: combined neurovascular injury
- ~~NV5: subtotal- or total amputation~~

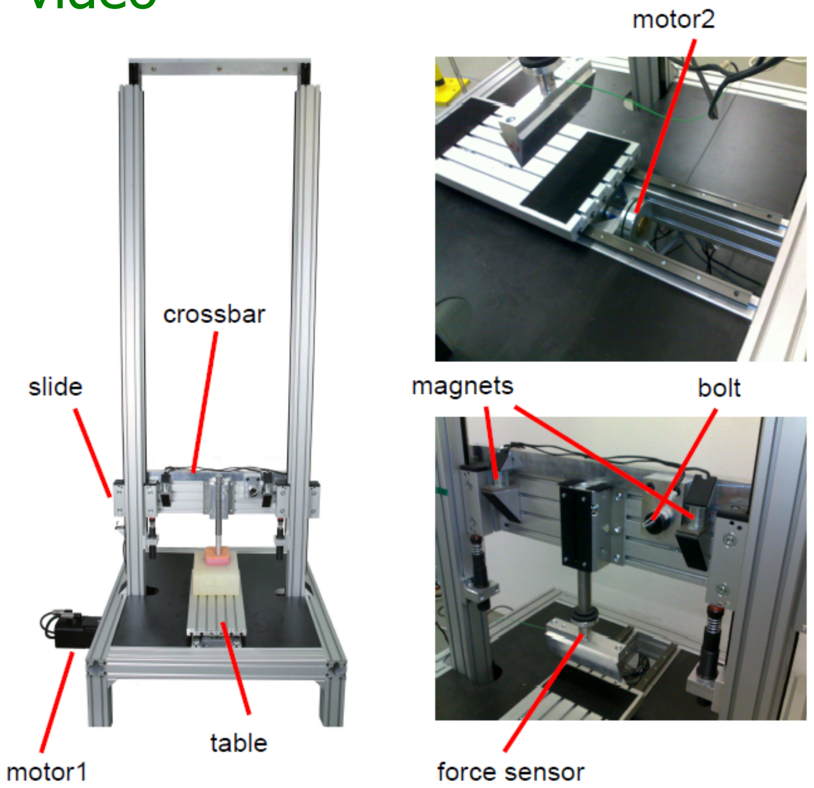




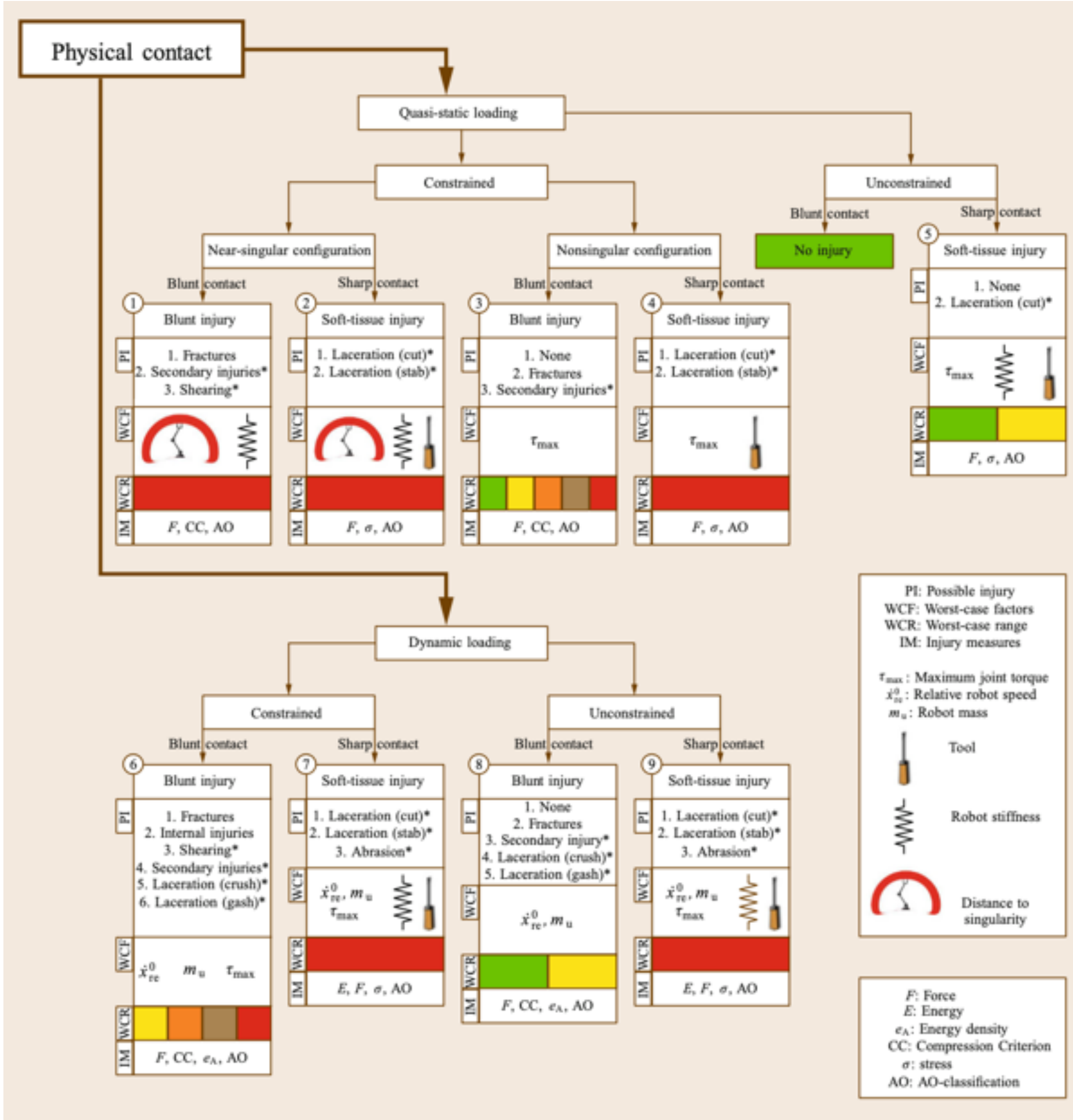
example:
IO2 MT2 NV4

Biomechanical tests

video

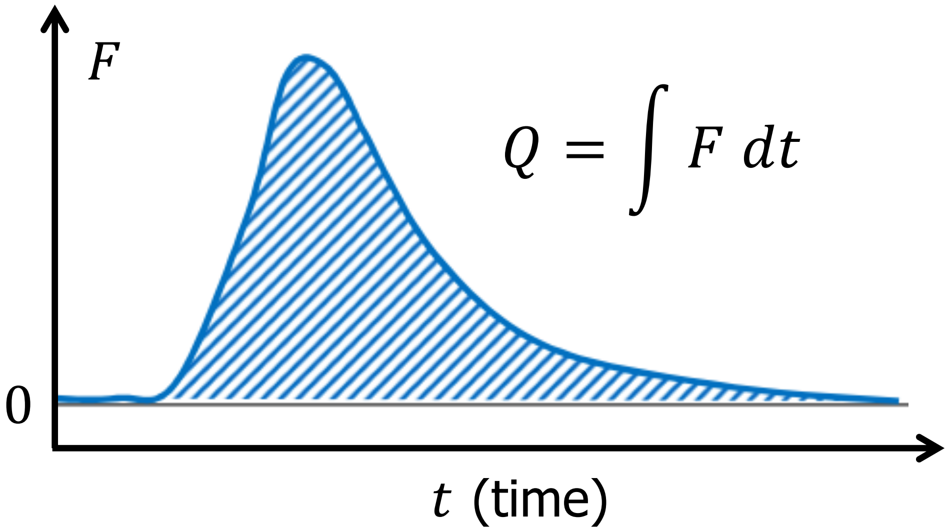


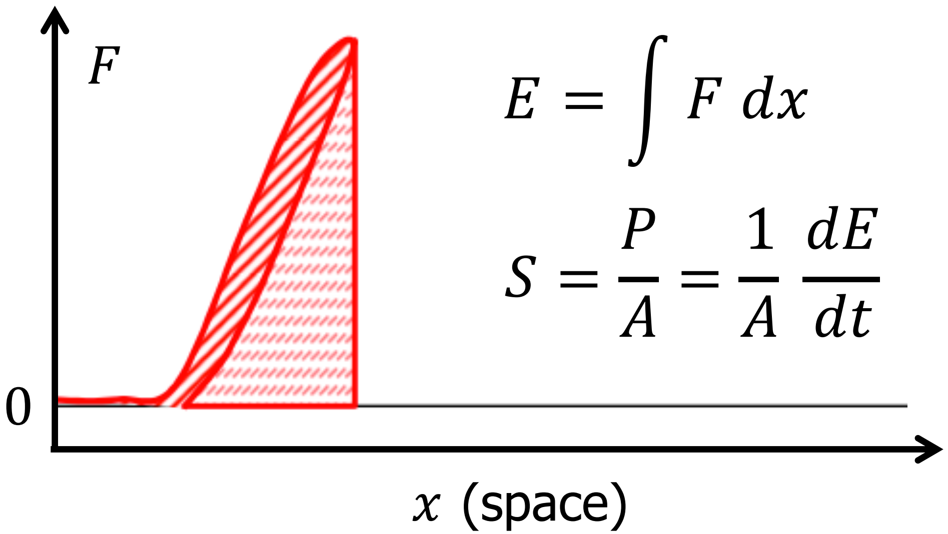
drop test impact measurements
on pig skin samples
+ medical evaluation at the
University Hospital –
Technical University of Munich (TUM)



Other measures

to assess transient limit criteria for impact severity

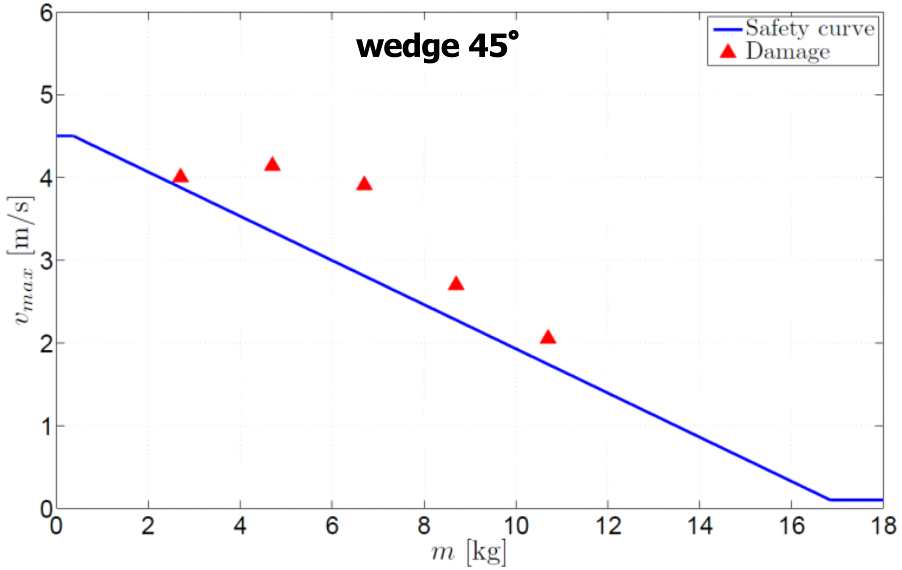


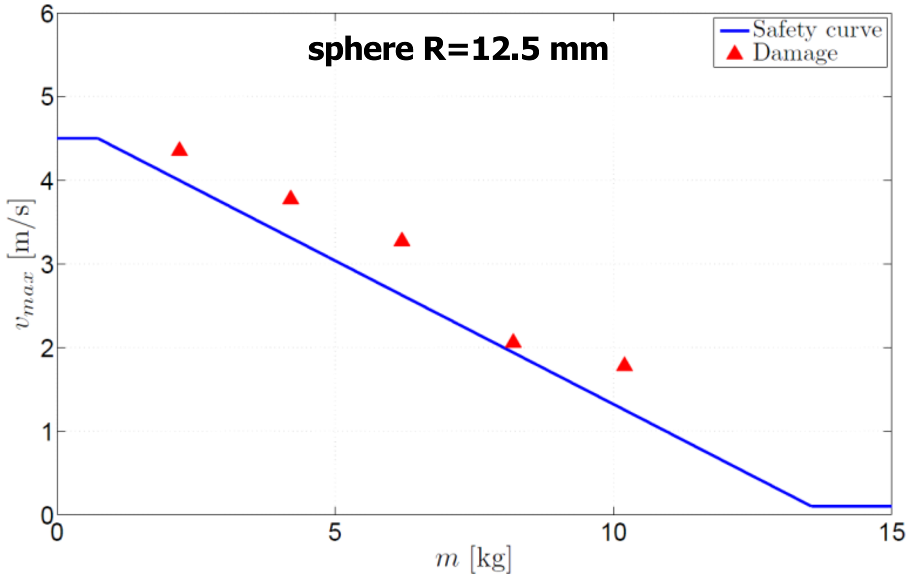


both for design and for control

- force F $[N]$
- contact area A $[m^2]$
- pressure p $[N/m^2]$
- momentum transfer Q $[kgm/s]$
- energy transfer E $[J]$
- power P $[W = J/s]$
- energy flux density K $[J/m^2]$
- power flux density S $[W/m^2]$

Maximum safe velocity

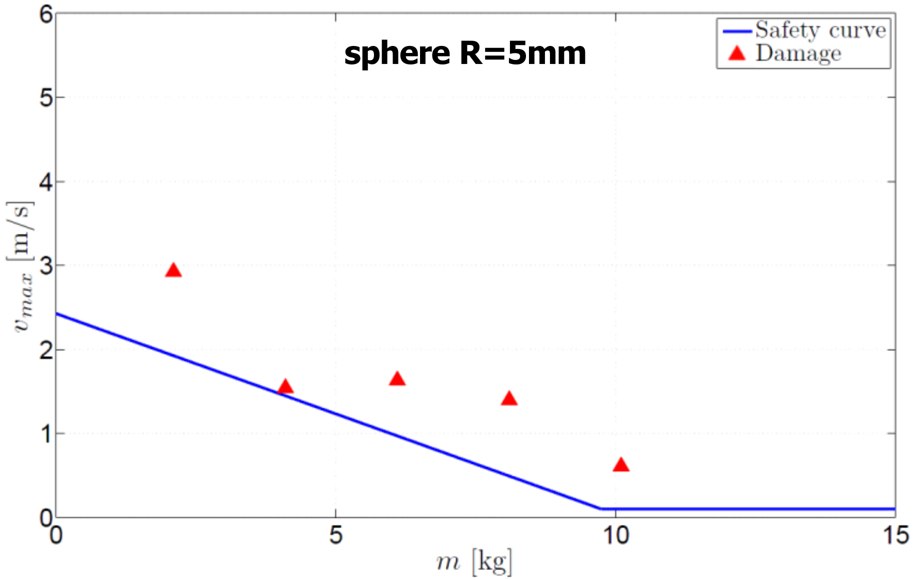




conservative limit curves/lines
on pairs (m [kg], $v_{\max}$ [m/s])
associated to key impacts conditions

inclusion of upper bounds to prevent
high speed close to a singularity

directional information related to task:
max (relative) speed, rather than velocity



Reflected inertia at the contact

the mathematics ...

dynamic model of rigid robot

$$M(q)\ddot{q} + S(q,\dot{q})\dot{q} + g(q) = \tau + (\tau_c = J_c^T(q)F_c)$$

robot inertia matrix ($M(q)$)

joint torque from external contact force (τ_c)

kinetic energy

$$T = \frac{1}{2}\dot{q}^T M(q)\dot{q}$$

analytic Jacobian of contact point

$$v_c = \dot{x}_c = J_c(q)\dot{q}$$

translational velocity only

robot inertia at contact point

$$\Lambda_c(q) = \left(J_c(q)\, M^{-1}(q)\, J_c^T(q)\right)^{-1} = J_c^{-T}(q)\, M(q)\, J_c^{-1}(q)$$

if Jacobian matrix is square and nonsingular

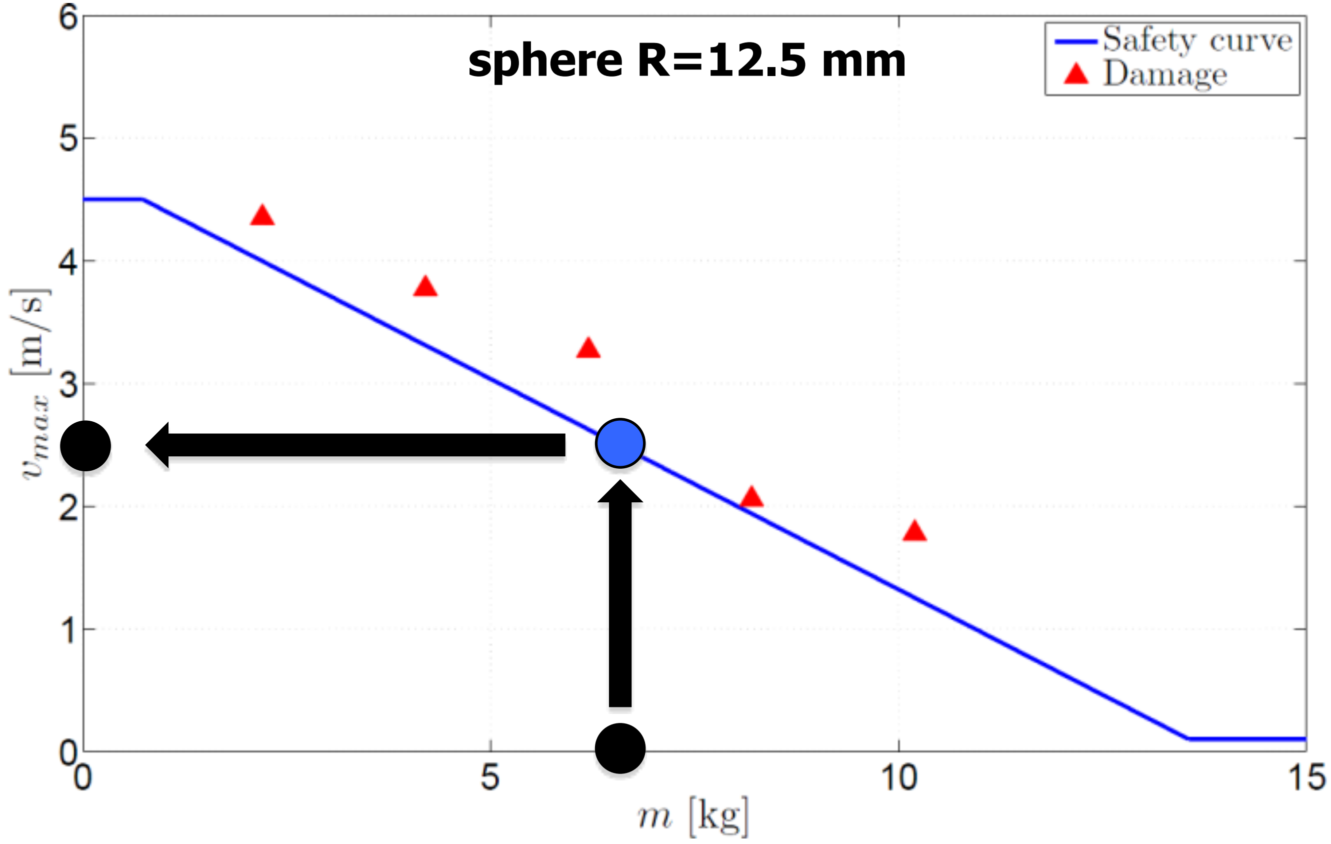
⇒ reflected robot inertia in unit direction $u \in \mathbb{R}^3$

$$m_R = \frac{1}{u^T \Lambda_c^{-1}(q) u}$$

... compliance may reduce the reflected inertia!

Maximum safe velocity

max safe velocity

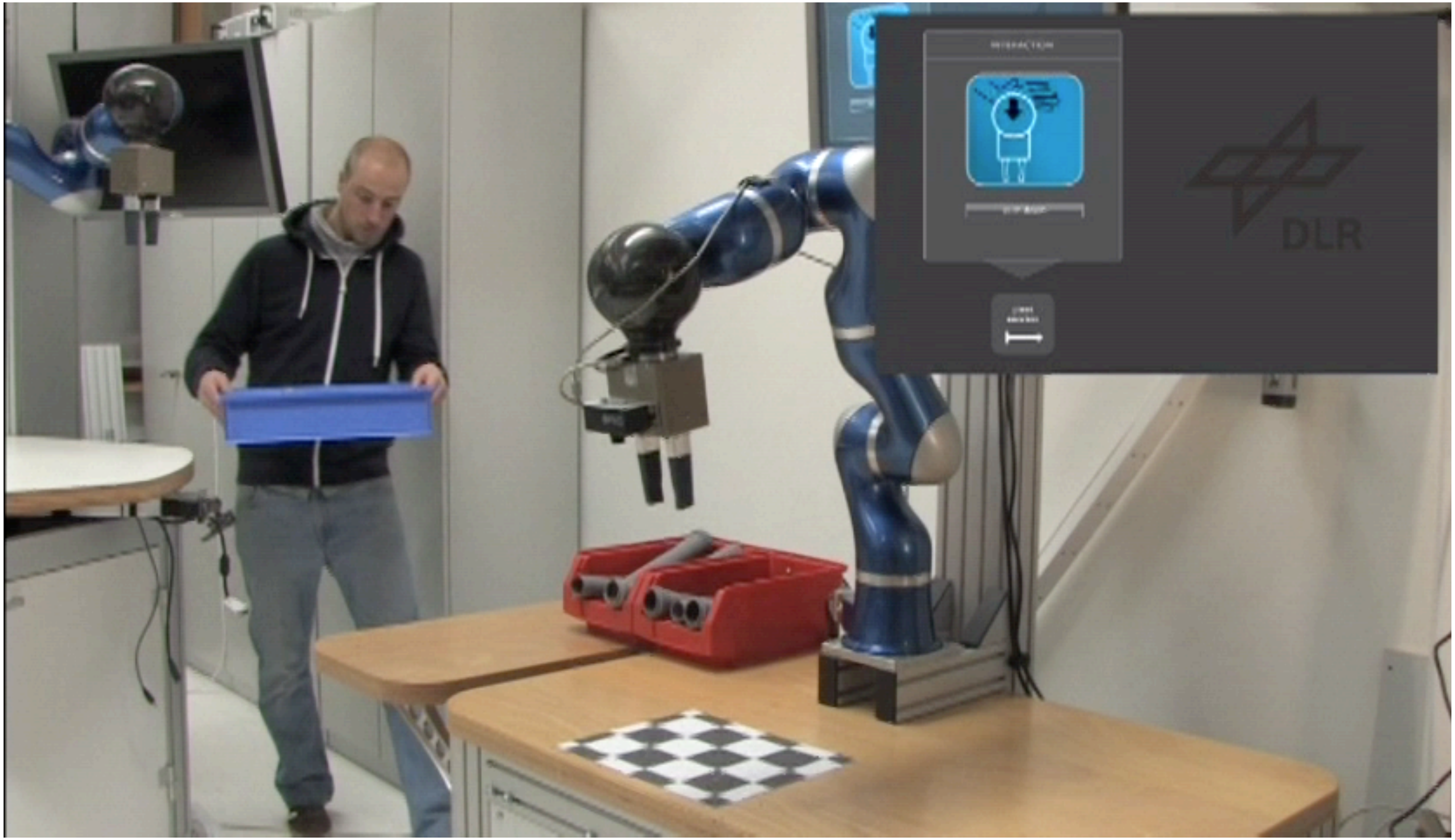


reflected **inertia**

video

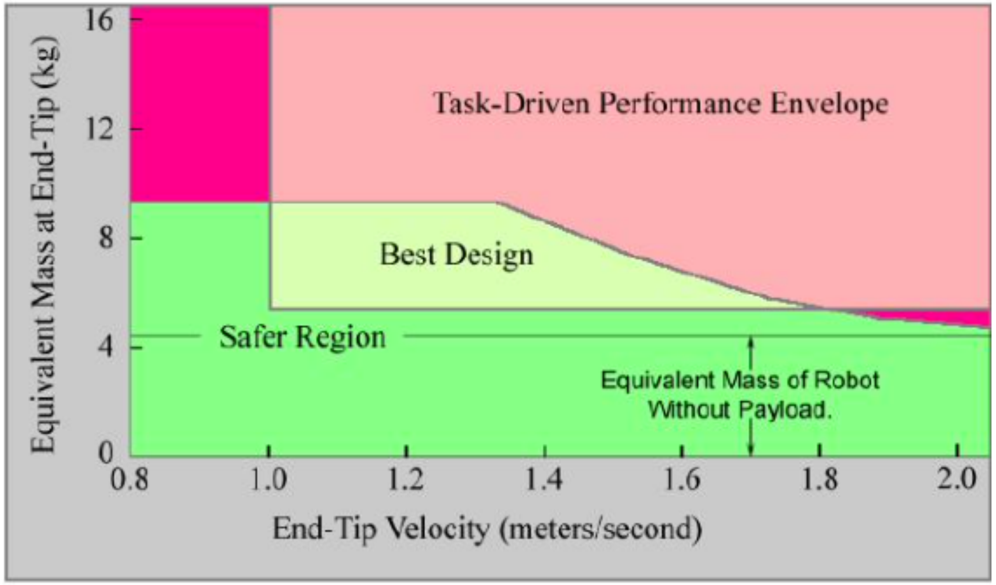
embedding injury knowledge into robot control: “ribbon” test

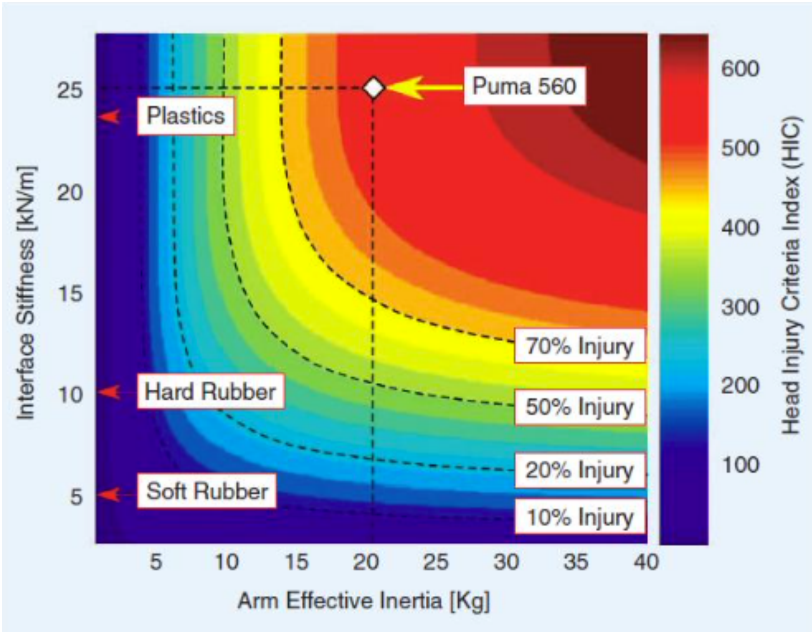
Robot reaction and HMI



video

Other biomechanical studies





$$\frac{E}{A} = \frac{mv^2}{2A} \approx \mathbf{2}\,\frac{J}{cm^2}$$

assuming $m = \mathbf{4}\,kg$, $v = \mathbf{1}\,\frac{m}{s}$, $A = \mathbf{1}\,cm^2$

$$HIC = T\left[\frac{1}{T}\int_0^T a(t)dt\right]^{2.5}$$

W. Townsend et al., Barrett Technologies
NASA Kennedy Space Center Report, May 1995

M. Zinn, O. Khatib et al., Stanford University
IEEE Robotics and Automation Mag., June 2004

and many more: University of Ljubljana, Fraunhofer IFF, University of Nagoya (Y. Yamada), …

Safety standards for industrial robots

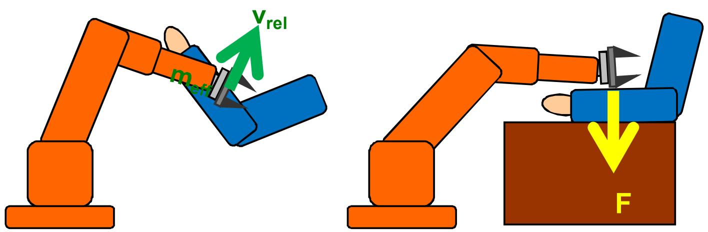

INTERNATIONAL STANDARD ISO 10218-1

Robots and robotic devices — Safety requirements for industrial robots —
Part 1:
Robots


INTERNATIONAL STANDARD ISO 10218-2

Robots and robotic devices — Safety requirements for industrial robots —
Part 2:
Robot systems and integration

- Safety Standards for Applications of Industrial Robots
  - ISO 10218-1, ISO 10218-2
  - Related standards and directives
- Safety Functions of Industrial Robot Controller
  - Review of basic safety-related functions
  - Supervision functions
- Present Standardization Projects
  - ISO/TS 15066 – Safety of collaborative robots
  - Biomechanical criteria
- Collaborative operation



several of the following (partly adapted) slides are
courtesy of B. Matthias, ABB Corporate Research

ISO standards 10218-1 and 10218-2

latest revisions ... :2011

ISO 10218-1

- Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots


INTERNATIONAL STANDARD
ISO 10218-1
Robots and robotic devices — Safety requirements for industrial robots —
Part 1:
Robots

- Scope
  - Industrial use
  - Controller
  - Manipulator
- Main references
  - ISO 10218-2 – Robot systems and integration

Common references

ISO 13849-1 / IEC 62061 – Safety-related parts of control systems

IEC 60204-1 – Electrical equipment (stopping fnc.)

ISO 12100 – Risk assessment

ISO 13850 – E-stop

ISO 10218-2

- Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration
- Scope
  - Robot (see Part 1)
  - Tooling
  - Work pieces
  - Periphery
  - Safeguarding


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

- Main references
  - ISO 10218-1 – Robot
  - ISO 11161 – Integrated manufacturing systems
  - ISO 13854 – Minimum gaps to avoid crushing
  - ISO 13855 – Positioning of safeguards
  - ISO 13857 – Safety distances
  - ISO 14120 – Fixed and movable guards

Related Standards and Directives

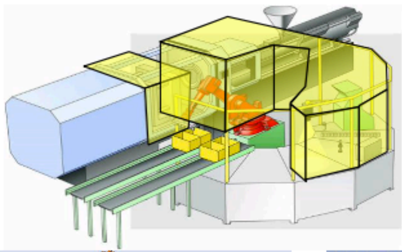
Type C Standards
- ISO 10218-2 – Robot system/cell
- ISO 10218-1 – Robot
- ISO/TS 15066 – Collaborative Robots

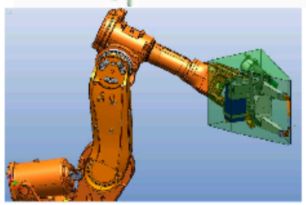
Type B Standards
- ISO 11161 – Integrated manufacturing systems
- EN ISO 13849-1:2008
- IEC 62061:2012

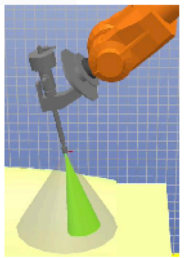
Type A Standards
- IEC 61508 – Functional Safety
- ISO 12100 – Risk Assessment

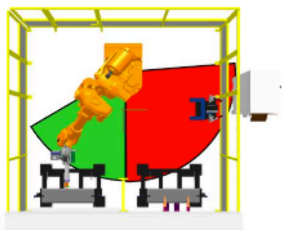
Laws + Directives
- Example EU: European Machinery Directive 2006/42/EC

Basic safety-related functions









- E-stop
- Protective stop
  - Stop categories (cat. 0, cat. 1, cat. 2 as per IEC 60204-1)
- Operating modes
  - Automatic / manual / manual high-speed
- Pendant controls
  - Enabling
  - Start / restart
  - Hold-to-run
- Limit switches
- Muting functions
  - Enable / limits switches / …

- Basic supervision of robot motion, i.e. motion executed corresponds to motion commanded
- Supervision of kinematic quantities
  - Position
    - TCPs, elbow, solid model of manipulator, tool
  - Speed
    - TCPs, elbow, …
  - Acceleration, braking
- Possibility: Supervision of dynamic quantities, esp. for collaborative operation
  - Torques
  - Forces
- Possibility: Application-related / user-defined supervision functions

ISO/TS Technical Specification 15066

ISO TC 184/SC 2 N
Date: 2010-10-12
ISO/PDTS 15066
ISO TC 184/SC 2/WG
Secretariat: SIS

Robots and robotic devices — Collaborative robots

Robots et equipment robotique — Robots collaboratives — Élément complémentaire

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TS = a normative document representing technical consensus within an ISO committee

Document type: Technical Specification
Document subtype:
Document stage: (30) Committee
Document language: E

D:\ISO\isomacroserver-prod\temp\DOCX2PDFISOTC\DOCX2PDFISOTC.SYSTEM@SRVWEB100_487\16339786_1.doc STD Version 2.1c

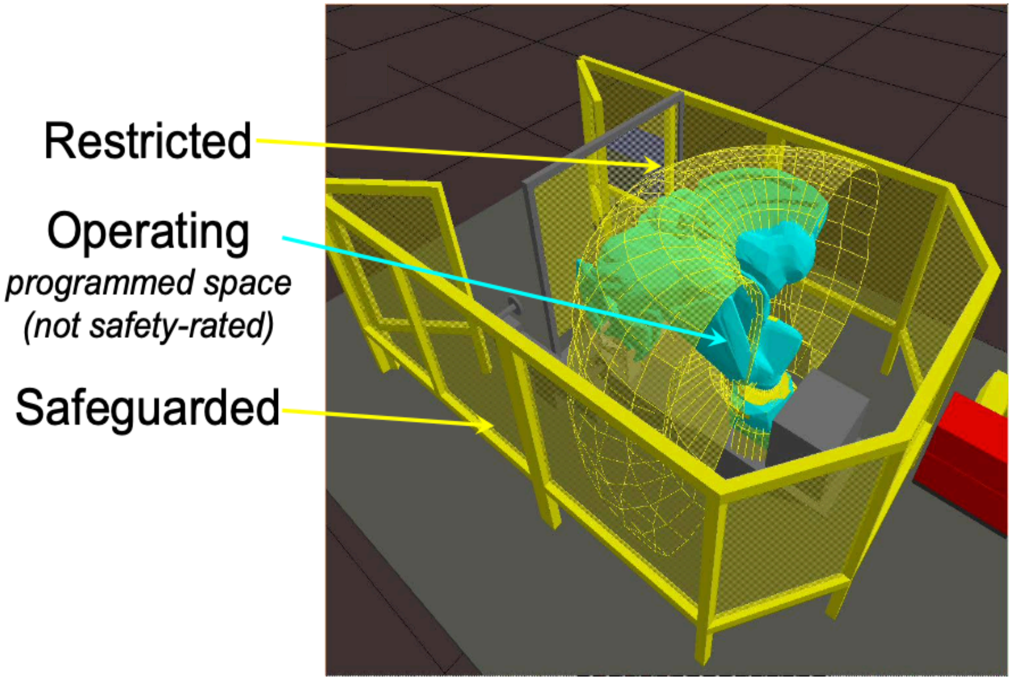
for collaborative robots

- Design of collaborative work space
- Design of collaborative operation
  - Minimum separation distance S / maximum robot speed K_R
  - Static (worst case) or dynamic (continuously computed) limit values
  - Safety-rated sensing capabilities
  - Ergonomics
- Methods of collaborative working
  - Safety-rated monitored stop
  - Hand-guiding
  - Speed and separation monitoring
  - Power and force limiting (biomechanical criteria!)
- Changing between
  - Collaborative / non-collaborative
  - Different methods of collaboration
- Operator controls for different methods, applications
  - Question is subject of debate: What if a robot is purely collaborative? Must it fulfill all of ISO 10218-1, i.e. also have mode selector, auto / manual mode, etc.?

latest version ... :2016

(reviewed and confirmed as such in 2019)

Robot spaces



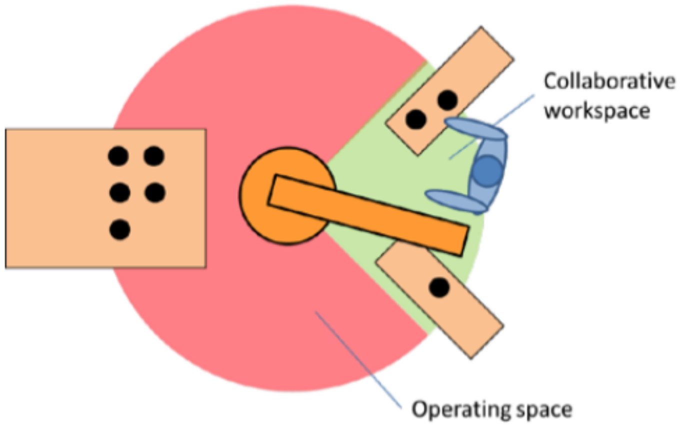
Maximum space
– space within which a robot system can move

Restricted space
– portion of the maximum space restricted by limiting devices that establish limits which will not be exceeded

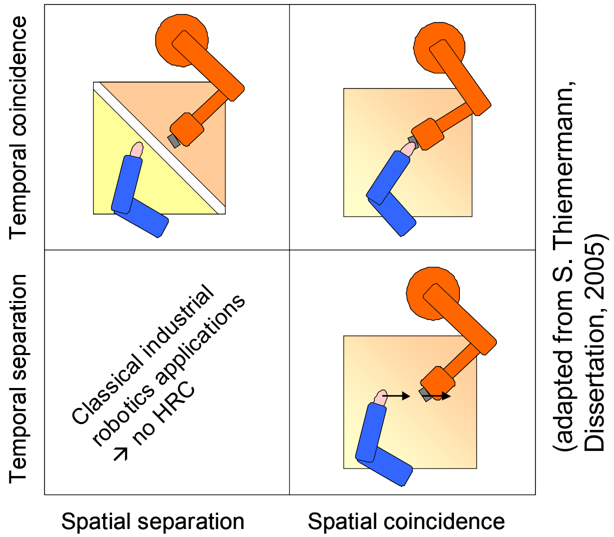
Operating space
– portion of the restricted space that is actually used while performing all motions commanded by the task program

Safeguarded space
– space defined by the perimeter safeguarding

true human-robot collaboration requires by-passing this last space!



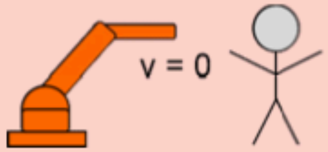
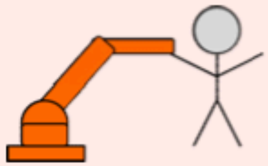
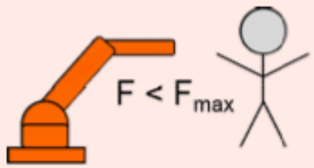
Definition of collaborative operation



- ISO 10218-1:2011, clause 3.4
  - ***collaborative operation***
    state in which purposely designed robots work in direct collaboration with a human within a defined workspace
- Degree of collaboration
  1. Once for setting up
     (e.g. lead-through teaching)
  2. Recurring isolated steps
     (e.g. manual gripper tending)
  3. Regularly or continuously
     (e.g. manual guidance)

Types of collaborative operation

according to ISO 10218-1, ISO/TS 15066

ISO 10218-1, clause	Type of collaborative operation	Main means of risk reduction	
5.10.2	Safety-rated monitored stop (Example: manual loading-station)	No robot motion when operator is in collaborative work space	
5.10.3	Hand guiding (Example: operation as assist device)	Robot motion only through direct input of operator	
5.10.4	Speed and separation monitoring (Example: replenishing parts containers)	Robot motion only when separation distance above minimum separation distance	
5.10.5	Power and force limiting by inherent design or control (Example: *ABB YuMi®* collaborative assembly robot)	In contact events, robot can only impart limited static and dynamics forces	

Types of collaborative operation

according to ISO 10218-1

	Speed	Separation distance	Torques	Operator controls	Main risk reduction
Safety-rated monitored stop	Zero while operator in CWS*	Small or zero	Gravity + load compensation only	None while operator in CWS*	No motion in presence of operator
Hand guiding	Safety-rated monitored speed (PL d)	Small or zero	As by direct operator input	E-stop; Enabling device; Motion input	Motion only by direct operator input
Speed and separation monitoring	Safety-rated monitored speed (PL d)	Safety-rated monitored distance (PL d)	As required to execute application and maintain min. separ. distance	None while operator in CWS*	Contact between robot and operator prevented
Power and force limiting	Max. determined by RA+ to limit impact forces	Small or zero	Max. determined by RA+ to limit static forces	As required for application	By design or control, robot cannot impact excessive force

* CWS = Collaborative Work Space　　+ RA = Risk Assessment

Emergency stop categories

Stop Categories according to IEC 60204-1 (NFPA79). Only Category 0 and 1 stops are allowed for the Estop.

- **Category 0 & 1** result in the removal of drive power, with Cat 0 being IMMEDIATE & Cat 1 being a controlled stop (decelerate then removal). With all UR robots, a Category 1 stop is a controlled stop where power is removed when a monitored standstill state is detected.
- **Category 2** is a stop where drive power is NOT removed. For Category 2 stops, this specification is defined in IEC 60204-1, A description of STO, SS1 and SS2 in IEC 61800-5-2.
  With UR robots, a Category 2 stop maintains the trajectory then retains power to the drives after stopping.

Any limit violation, or fault detected in a safety function, results in a Category 0 stop.

SF #	Safety Function	Description	PFHd	What is controlled
1	**Emergency Stop** 1, 2, 3	Pressing the Estop PB on the pendant[1] or the External Estop (if using the Estop Safety Input) results in a Cat 1 stop[3]. Command[1] all joints to stop and upon all joints coming to a monitored standstill state, power is removed. This is a Cat 1 stop[3]. See Stop Time and Stop Distance Safety Functions[4] and the User Manual.	**1.30E-07**	**Robot**
2	**Safeguard Stop** (Protective Stop according to ISO 10218-1)	This safety function is initiated by an external protective device using safety inputs which will initiate a Cat 2 stop[3]. See the Stop Time and Stop Distance Safety Functions[4] and the User Manual. *For the functional safety of the complete integrated safety function, add the PFHd of the external protective device to the PFHd of the Safeguard Stop.*	**1.20E-07**	**Robot**

UNIVERSAL ROBOTS

UR e-Series Safety Functions and Safety I/O

Types of collaborative operation - 1

Safety-rated monitored stop
(ISO 10218-1, 5.10.2, ISO/TS 15066)

- Reduce risk by ensuring robot standstill whenever a worker is in collaborative workspace
- Achieved by
  - Supervised standstill - Category 2 stop (IEC 60204-1)
  - Category 0 stop in case of fault (IEC 60204-1)
- Application
  - Manual loading of end-effector with drives energized
  - Automatic resume of motion

Hand guiding
(ISO 10218-1, 5.10.3, ISO/TS 15066)

- Reduce risk by providing worker with direct control over robot motion at all times in collaborative workspace
- Achieved by (controls close to end-effector)
  - Emergency stop, enabling device
  - Safety-rated monitored speed
- Application
  - Ergonomic work places
  - Coordination of manual + partially automated steps

Safety-rated monitored stop

allows direct operator-robot system interaction under specific conditions

- safety-rated stop condition before operator enters collaborative workspace
- drive power remains ON
- motion resumes after operator leaves workspace
  - robot motion resumes without additional action
- protective stop issued if stop condition is violated
- used with other collaborative modes of operation

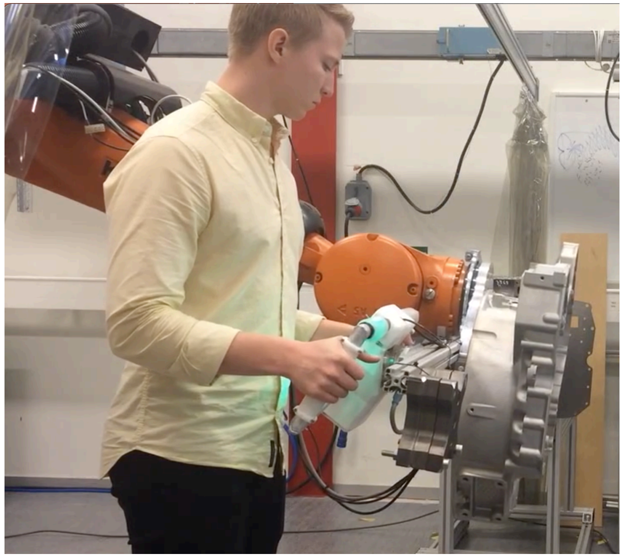
Robot <system> motion or stop function		Operator’s proximity to collaborative workspace	
		Outside	Inside
Robot’s <system> proximity to collaborative workspace	Outside	Continue	Continue
	Inside and moving	Continue	Protective stop
	Inside, at Safety-Rated Monitored Stop	Continue	Continue

Hand guiding

operator uses a hand-operated device to transmit motion commands

- BEFORE the operator enters the collaborative workspace, the robot achieves a safety-rated monitored stop
  - drive power remains ON
- operator grasps a hand-operated device (it includes also an enabling device), activating motion/operation
- non-collaborative operation resumes when the operator leaves
- highly variable uses: it acts like a manual "tool"

robotic lift assist

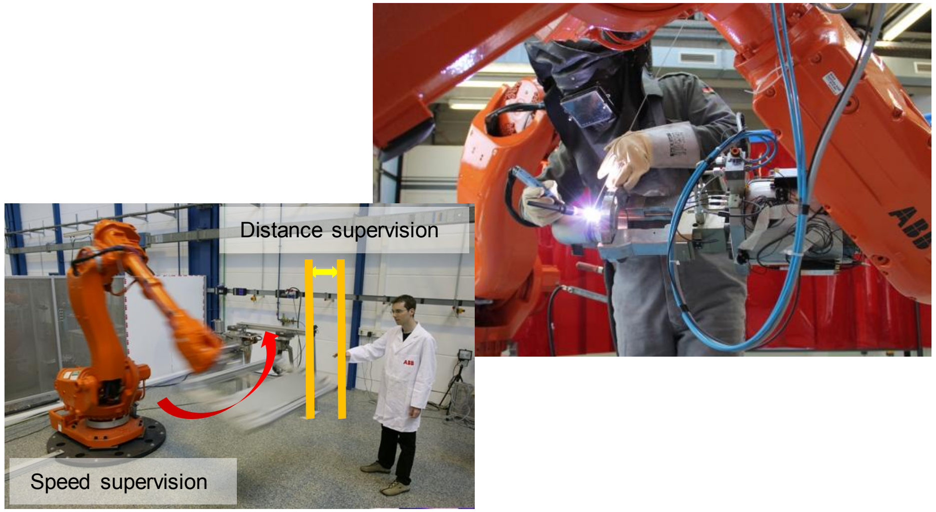


used in automatic mode not for teaching

Types of collaborative operation - 2

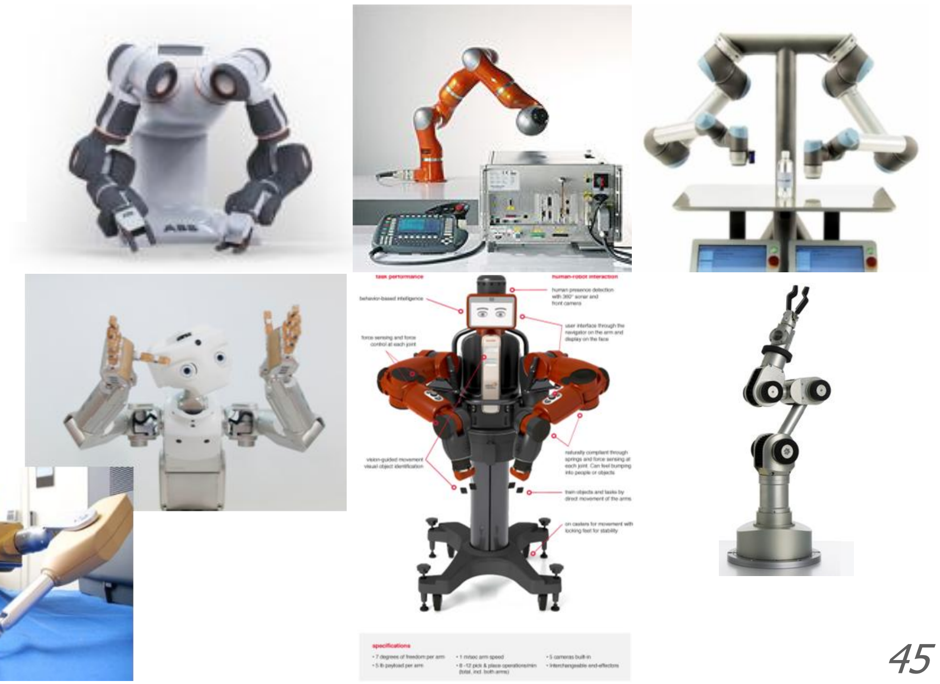
Speed and separation monitoring
(ISO 10218-1, 5.10.4, ISO/TS 15066)

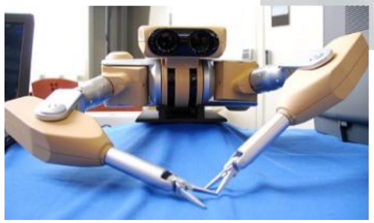
- Reduce risk by maintaining sufficient distance between worker and robot in collaborative workspace
- Achieved by
  - distance supervision, speed supervision
  - protective stop if minimum separation distance or speed limit is violated
  - taking account of the braking distance in minimum separation distance
- Additional requirements on safety-rated periphery
  - for example, safety-rated camera systems



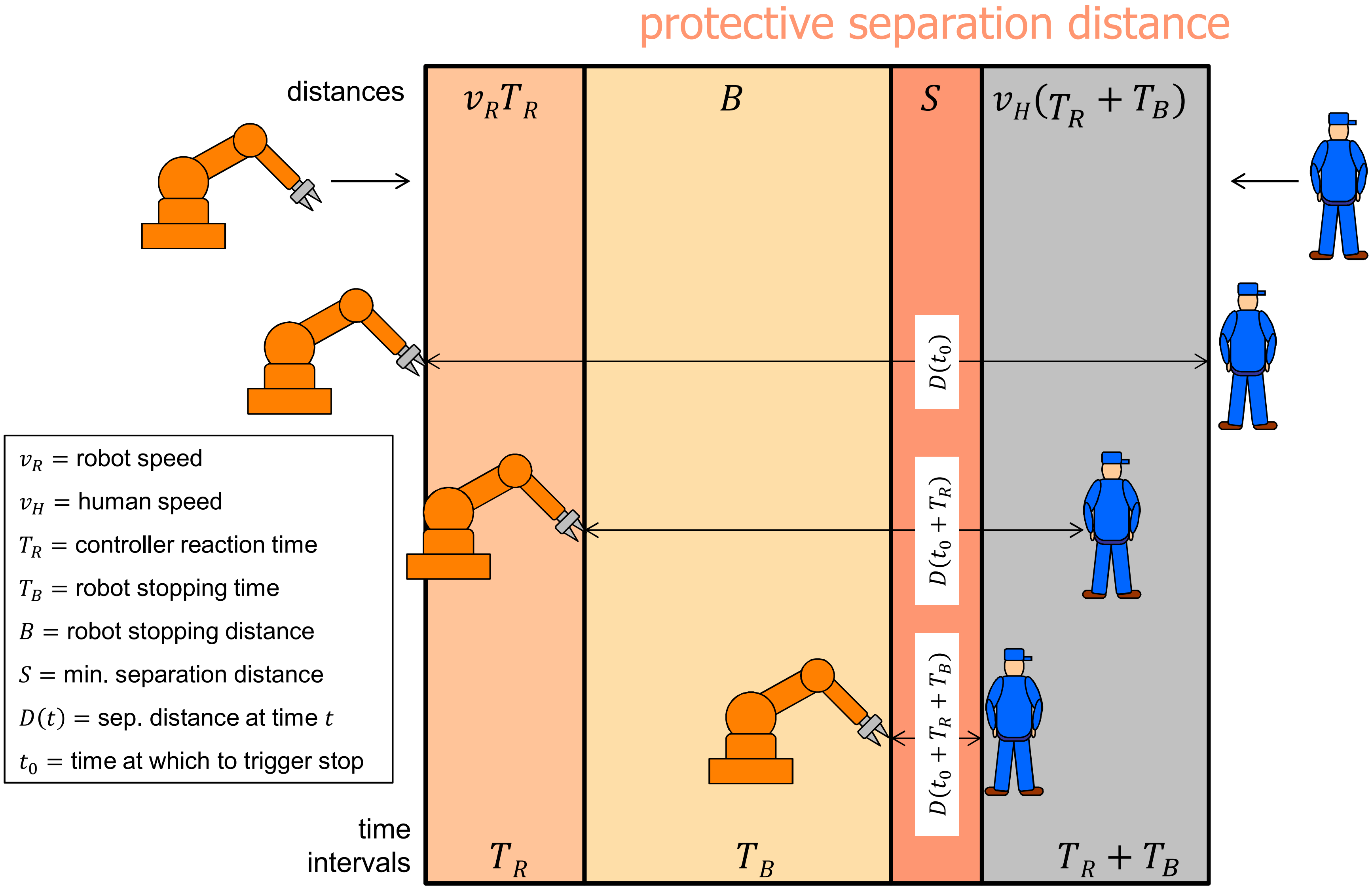
Power and force limiting by inherent design or control
(ISO 10218-1, 5.10.5, ISO/TS 15066)

- Reduce risk by limiting mechanical loading of human-body parts by moving parts of robot, end-effector or work piece
- Achieved by low inertia, suitable geometry and material, control functions, …
- Applications involving transient and/or quasi-static physical contact (SPA = small parts assembly)





Speed and separation monitoring



Speed and separation monitoring

intrusion distance (ISO 13855)

protective separation distance

uncertainties robot + distance sensor

$$S_{protective}(t_0) = S_{human} + S_{reaction} + S_{stopping} + C + Z_r + Z_d$$

$$S_{human} = \int_{t_0}^{t_0+T_r+T_s} v_H(t)\, dt$$

$$S_{reaction} = \int_{t_0}^{t_0+T_r} v_R(t)\, dt$$

$$S_{stopping} = \int_{t_0+T_r}^{t_0+T_r+T_s} v_R(t)\, dt$$

Here, $t_0 =$ “now” and $t =$ integration variable.

Condition for sufficient protection at t_0 is
$S_{measured}(t_0) \geq S_{protective}(t_0)$

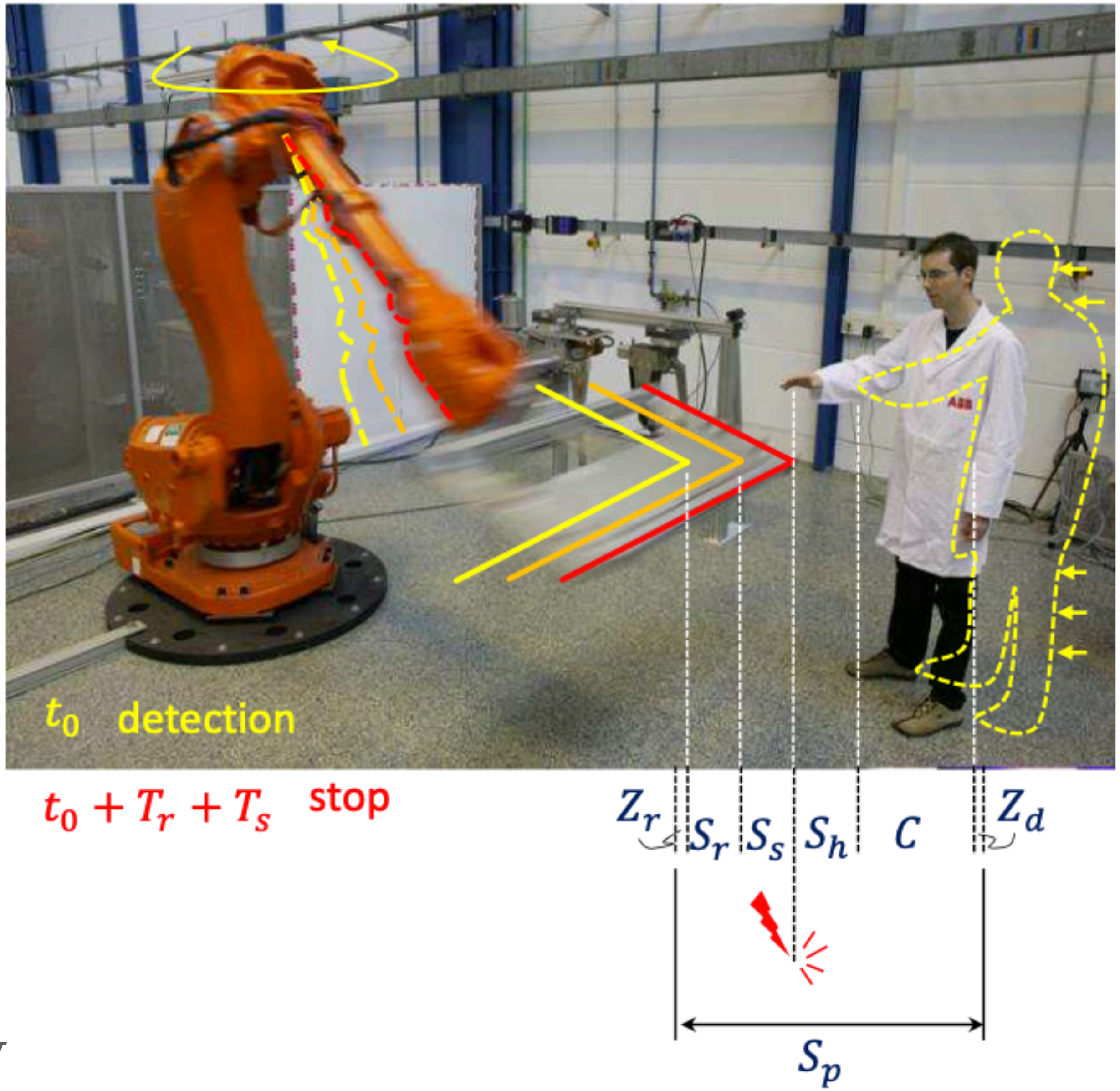
Simple model assumptions (constant values) for $v_H(t)$ and for $v_R(t)$ in the reaction-phase of the robot motion can be made to give:

$$S_{human} = v_H(t_0) \cdot (T_r + T_s)$$

$$S_{reaction} = v_R(t_0) \cdot T_r$$

Values for the stopping distance $S_{stopping}$ should be obtained, as stated, from the data provided according to ISO 10218-1, Annex B

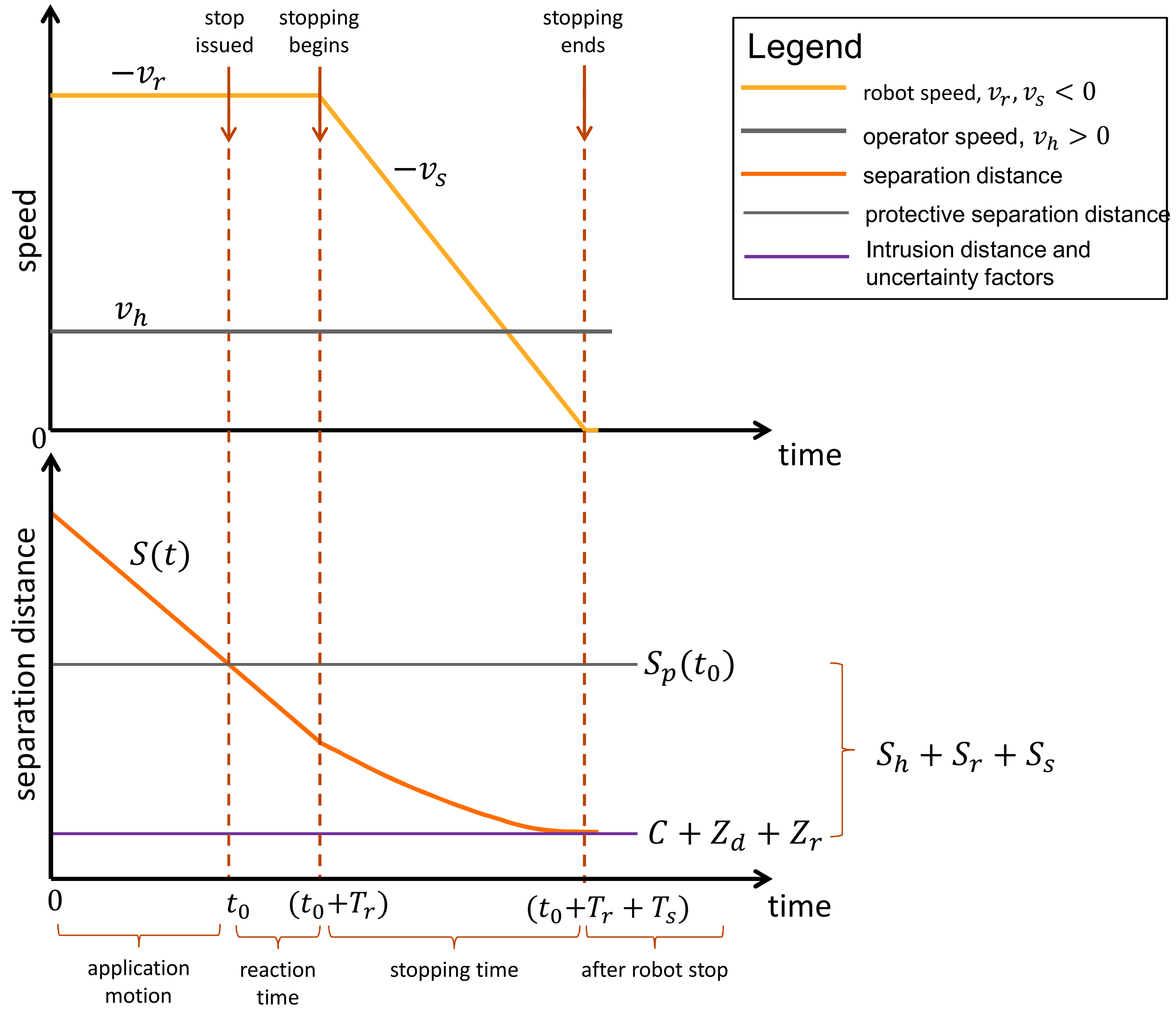
Speed and separation monitoring



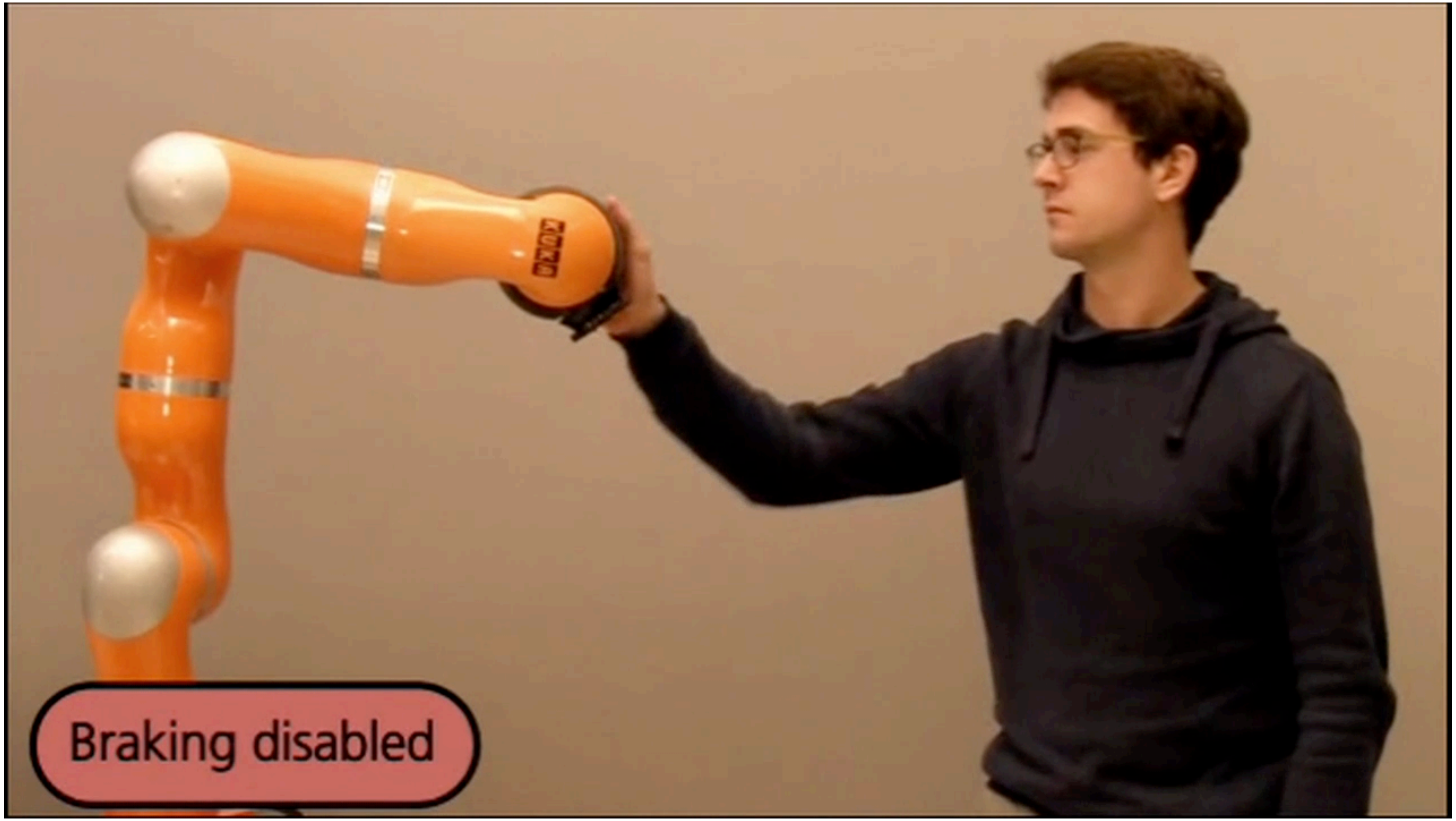
protective separation distance S_p

$$S_p = S_r + S_s + S_h + Z_r + C + Z_d$$

Speed and separation monitoring

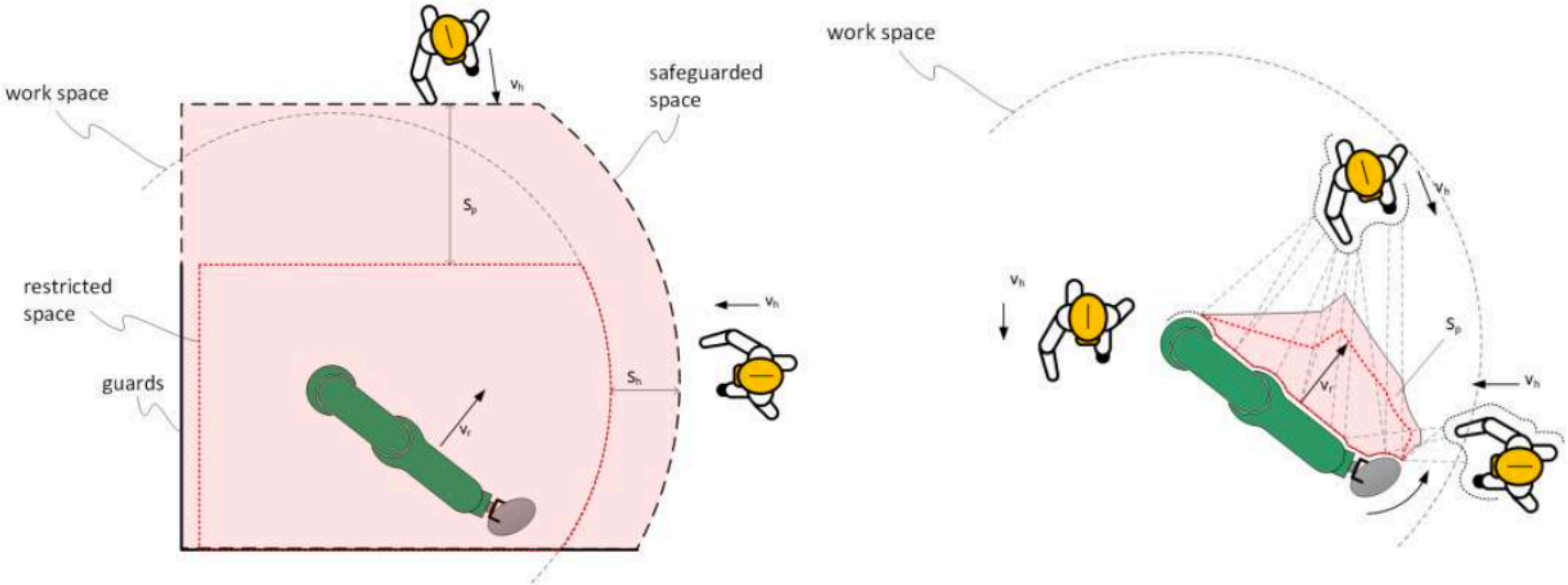


Stopping a LWR arm …
having joint compliance



Safeguarding and collaborative SSM

a simple comparison



- perimeter safeguarding with limited (slow) speed is not a collaborative mode
- presence sensing is a measure to prevent restart

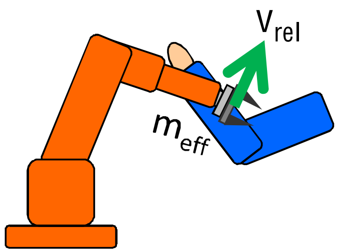
- continuous localization and computation of distances
- frequent access, automatic restart

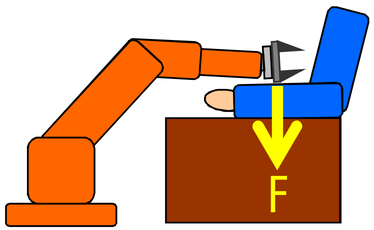
courtesy of F. Vicentini CNR-STIIMA

Power and force limiting

- types of contact events for robot systems specifically designed for power and force limiting
- robot-workpiece-human contacts can occur intentionally or not

<table>
<tr><td></td><td colspan="4">ISO / TS 15066 – clause 5.4.4 “Power and force limiting”</td><td></td></tr>
<tr><td></td><td colspan="2">Free impact / transient contact
• Contact event is “short” (< 50 ms)
• Human body part can recoil</td><td colspan="2">Constrained contact / quasi-static contact
• Contact duration is “extended”
• Human body part cannot recoil, is trapped</td><td></td></tr>
<tr><td>use of impact models</td><td colspan="2">Accessible parameters in design or control
• Effective mass (robot pose, payload)
• Speed (relative)</td><td colspan="2">Accessible parameters in design or control
• Force (joint torques, pose)</td><td>extra sensors</td></tr>
<tr><td rowspan="2">bio-mechanical studies</td><td>Pain threshold</td><td>Minor injury threshold</td><td>Pain threshold</td><td>Minor injury threshold</td><td></td></tr>
<tr><td>Highest loading level accepted in design</td><td>Highest loading level accepted in risk assessment in case of single failure</td><td>Highest loading level accepted in design</td><td>Highest loading level accepted in risk assessment in case of single failure</td><td></td></tr>
</table>



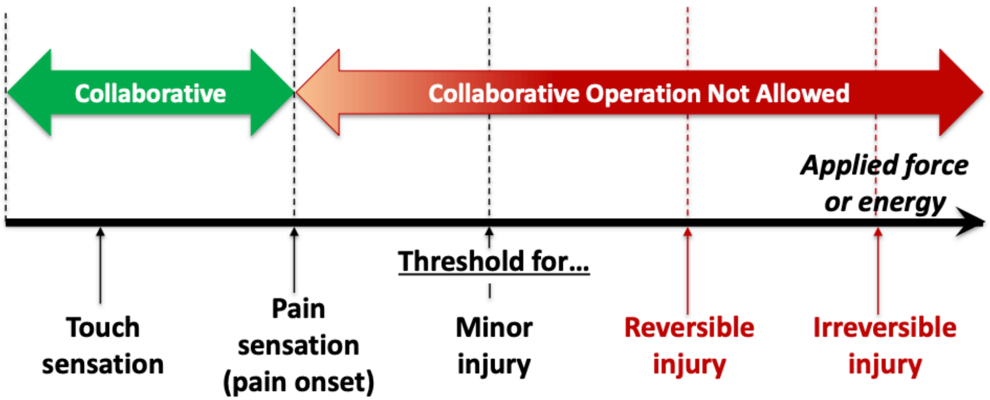


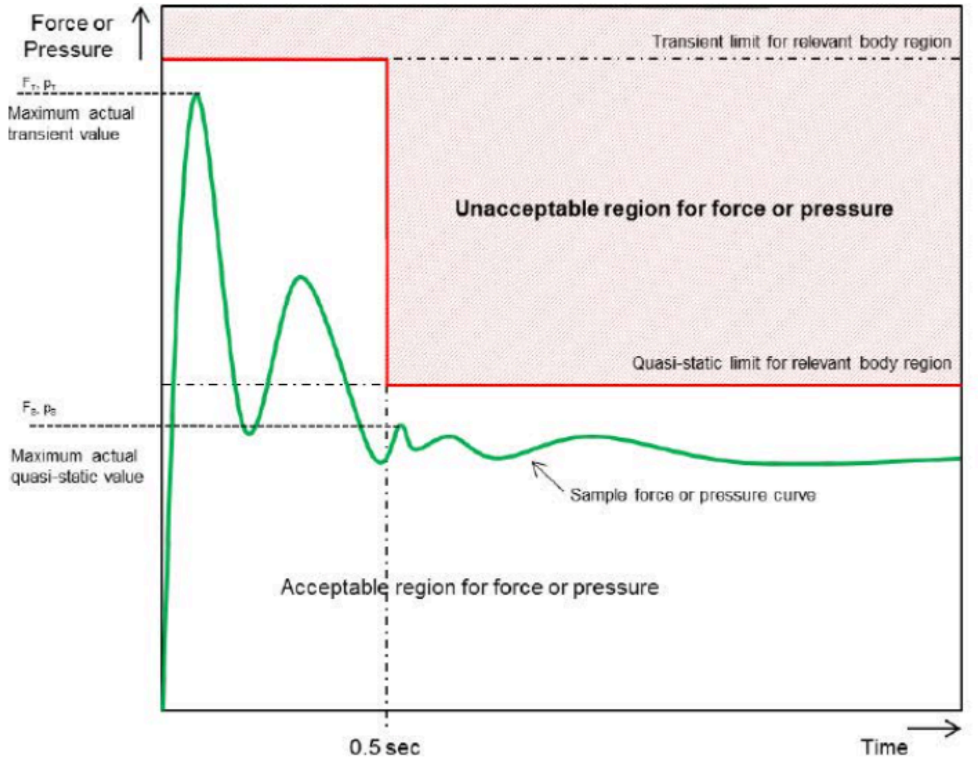
Biomechanical criteria in TS 15066

$80\ W/150\ N$ power and force limits were present in ISO 10218-1:2006 but have been removed in 2011!

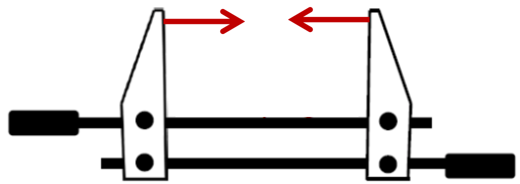
$$1\ W = 1\ N\frac{m}{s} = 1\frac{kg\ m^2}{s^3}$$

"onset of pain" studies

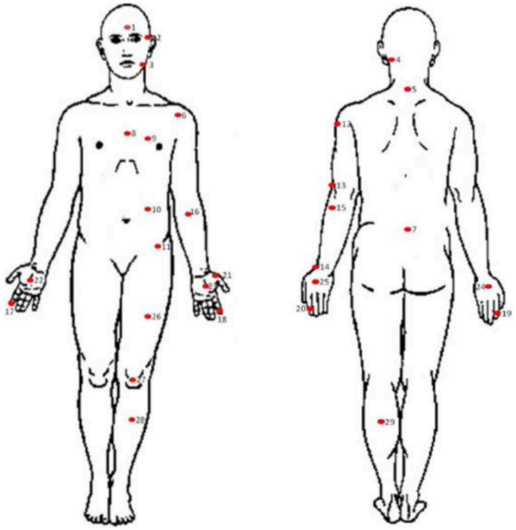




- force applied where (body part)?
- clamping conditions?



Biomechanical criteria in TS 15066

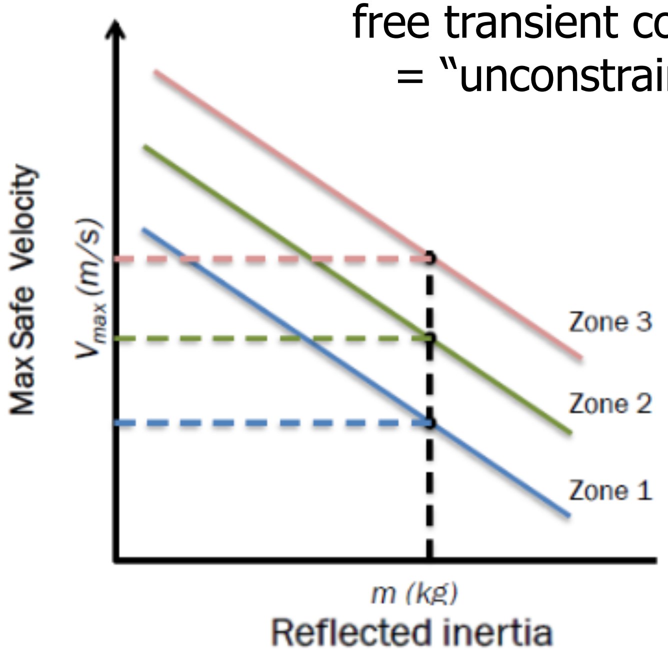


Body Region		Specific Body Area	Quasi-Static Contact: Maximum Allowable Pressure p_s [N/cm2] (see NOTE 1)	Quasi-Static Contact: Maximum Allowable Force [N] (see NOTE 2)	Transient Contact: Maximum Allowable Pressure Multiplier P_T (see NOTE 3)	Transient Contact: Maximum Allowable Force Multiplier F_T (see NOTE 3)
Skull and forehead	1	Middle of forehead	125	130	N/A	N/A
	2	Temple	112		N/A	
Face	3	Masticatory muscle	110	65	N/A	N/A
Neck	4	Neck muscle	138	145	2	2
	5	Seventh neck muscle	205		2	
Back and shoulders	6	Shoulder joint	155	210	2	2
	7	Fifth lumbar vertebra	213		2	2
Chest	8	Sternum	116	140	2	2
	9	Pectoral muscle	166		2	
Abdomen	10	Abdominal muscle	143	110	2	2
Pelvis	11	Pelvic bone	209	180	2	2
Upper arms and elbow joints	12	Deltoid muscle	192	150	2	2
	13	Humerus	216		2	
Lower arms and wrist joints	14	Radial bone	192	160	2	2
	15	Forearm muscle	181		2	
	16	Arm nerve	179		2	
Hands and fingers	17	Forefinger pad D	298	135	2	2
	18	Forefinger pad ND	273		2	
	19	Forefinger end joint D	275		2	
	20	Forefinger end joint ND	219		2	
	21	Thenar eminence	203		2	
	22	Palm D	256		2	
	23	Palm ND	260		2	
	24	Back of the hand D	197		2	
	25	Back of the hand ND	193		2	
Thighs and knees	26	Thigh muscle	246	220	2	2
	27	Kneecap	223		2	
Lower legs	28	Middle of shin	220	125	2	2
	29	Calf muscle	212		2	

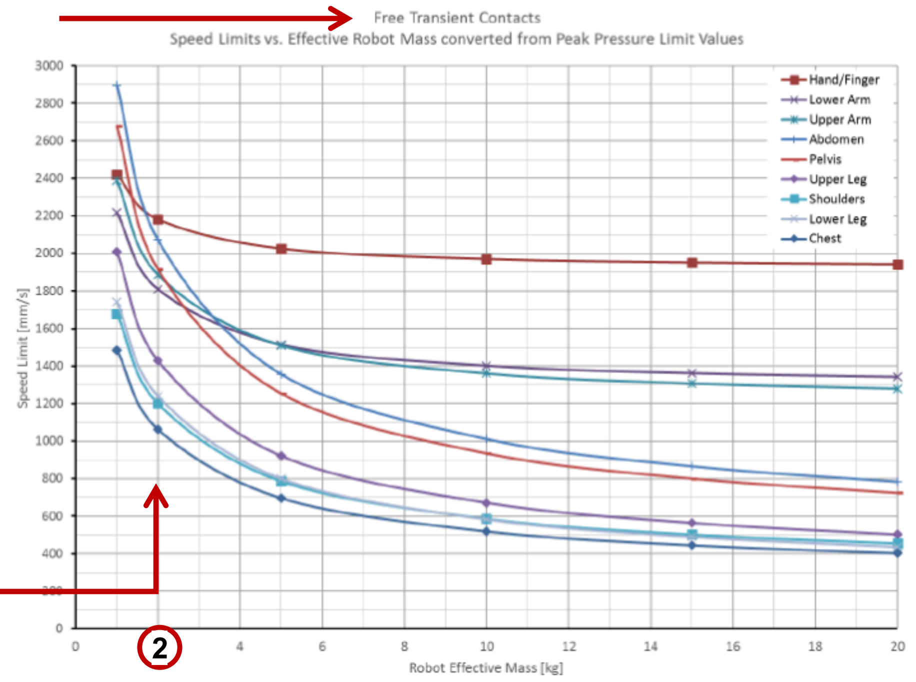
CRITICAL ZONE

from studies by the University of Mainz

Biomechanical criteria in TS 15066



free transient contacts
= "unconstrained"



body parts

… from the Handbook of Injury in SAPHARI

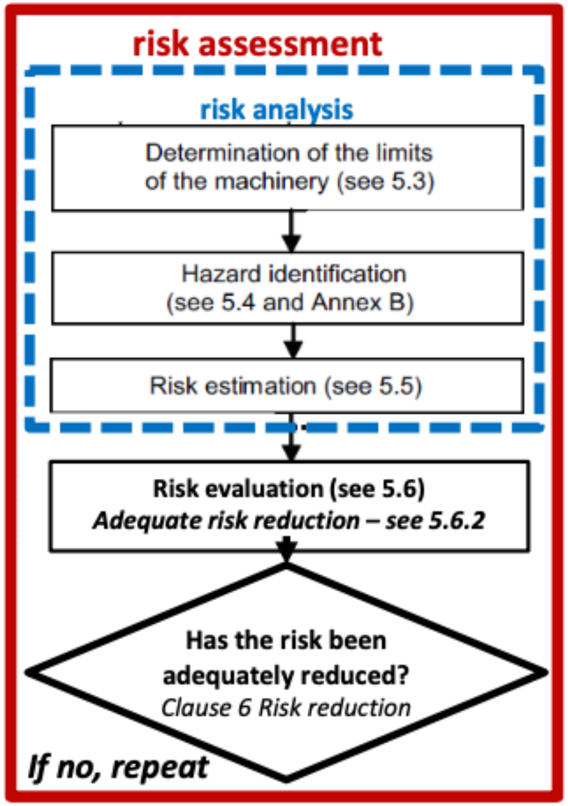
Body region	Speed limit [mm/sec] as a function of robot effective mass (m_R) based on maximum pressure value (p_{max}) with an area (A) of 1 cm²					
	1	2	5	10	15	20
Hand/finger	2 400	2 200	2 000	2 000	2 000	1 900
Lower arm	2 200	1 800	1 500	1 400	1 400	1 300
Upper arm	2 400	1 900	1 500	1 400	1 300	1 300
Abdomen	2 900	2 100	1 400	1 000	870	780
Pelvis	2 700	1 900	1 300	940	800	720
Upper leg	2 100	1 500	1 000	810	730	680
Lower leg	1 900	1 400	1 000	900	840	810
Shoulders	1 700	1 200	790	590	500	450
Chest	1 500	1 100	700	520	440	400

SAPHARI
Safe and Autonomous Physical Human-Aware Robot Interaction

Risk assessment

risk assessment in evaluating a HRC application

Source: ISO 12100:2010 – Safety of machinery



- use case (tasks) identification
- hazard identification
- risk estimation
- risk reduction
- iterate until acceptable residual risk

RISK REDUCTION – *Table 2 without E0*

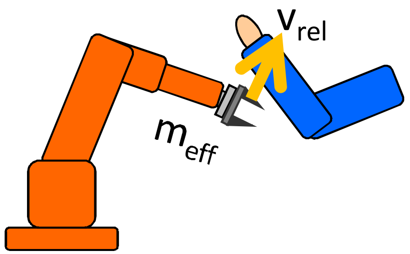
Severity	EXPOSURE	Probability of AVOIDANCE	Risk Level
S1 Minor	E1 low	A1 likely	Negligible
		A2 or A3 not likely or not possible	Low
	E2 high		Low
S2 Moderate	E1 low		Medium
	E2 high	A1 likely	Medium
		A2 or A3 not likely or not possible	High
S3 Serious	E1 low		High
	E2 high	A1 or A2 likely or not likely	High
		A3 not possible	Very High

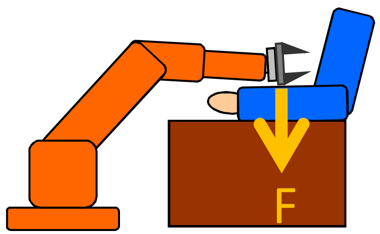
Risk Reduction Measure	Risk Level: VERY HIGH / HIGH / MEDIUM	LOW / NEGLIGIBLE
Elimination Substitution Limit Interaction	Use of 1 or a combination of these risk reduction measures are required as a primary means to reduce risks.	Use of one or a combination of any of the risk reduction measures that would reduce risks to an acceptable level may be used.
Safeguarding/ SRP/CS		
Complementary Protective Measures	Use of one or a combination of these risk reduction measures may be used in conjunction with the above risk reduction measures but shall not be used as the primary risk reduction measure.	
Warnings and Awareness Means		
Administrative Controls		
PPE		

Basic hazards for contact events

ISO/TS 15066 – clause 5.5.4 “Power and force limiting”

	Transient Contact	**Quasi-Static Contact**
Description	• Contact event is “short” (< 50 ms) • Human body part can usually recoil	• Contact duration is “extended” • Human body part cannot recoil, is trapped
Limit Criteria	• Peak forces, pressures, stresses • Energy transfer, power density	• Peak forces, pressures, stresses
Accessible in Design or Control	• Effective mass (robot pose, payload) • Speed (relative) • Contact area, duration	• Force (joint torques, pose) • Contact area, duration

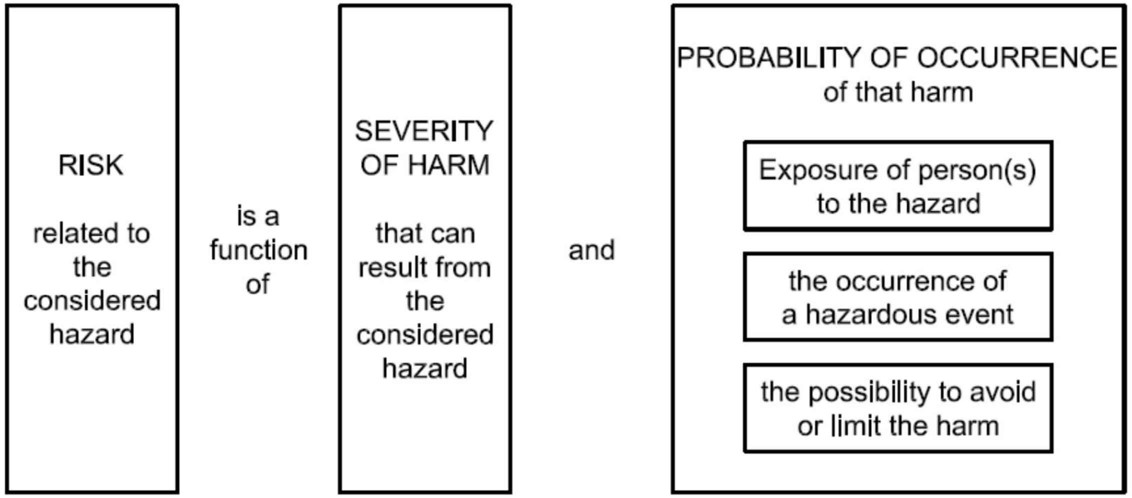




Risk estimation and reduction

risk estimation process

for each single hazard and combined



risk reduction measures

exemplified

Most preferred → *Least preferred*

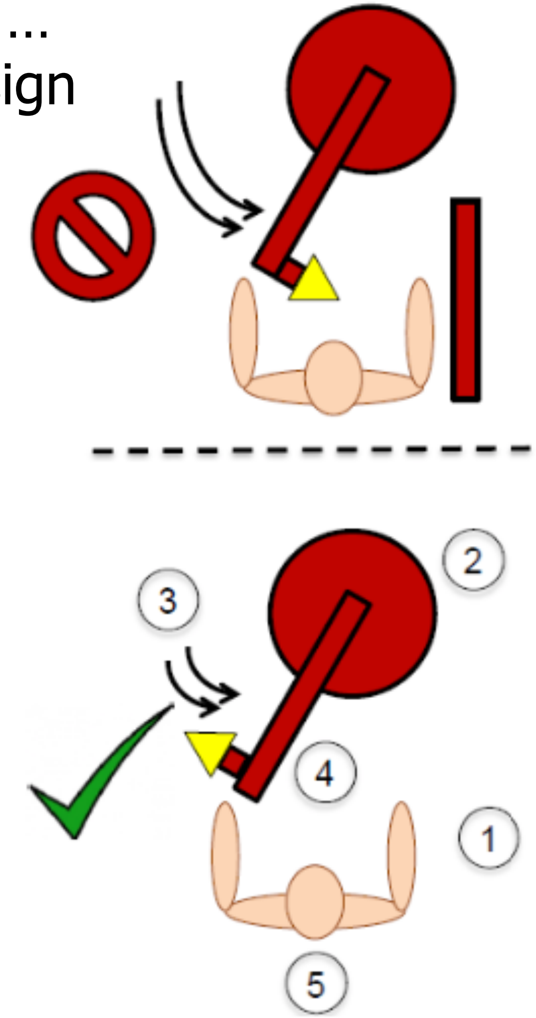
Inherently Safe Design Measures			Safeguarding & Complementary Protective Measures		Information for Use		
Elimination	**Substitution**	**Limit Interaction**	**Safeguard**	**Comp Protective Measures**	**Warnings & Awareness Means**	**Administrative (organizational) Controls**	**PPE**
Process or layout design, redesign or modification	• Less hazardous materials • Intrinsically safe • Reduce energy • …	• Eliminate or reduce human interaction • Automate tasks • Modify layout or process flow • …	• Guards • Interlocks • Protective Devices • Safety controls, logic & functions • Safety parameters & configurations • …	• Fall prevention • Escape & rescue • Safe access • Safe handling • Energy isolation • Enabling devices • Estops …	• Lights, beacons and strobes • Audible alarms • Signs, labels or markings	• Training and SOPs • Inspections • Rotation of workers • Changing schedules • Control of Haz Energy • HazCom • Confined Space • Management	Clothing, footwear, glasses, respirators, gloves & more for specific safety purposes

Examples of risks and mitigation plan

Item	Risks	Mitigation plan
Sensing	sensor not safety certified	use of redundant heterogeneous sensors
	unreliable skin sensor measurements	proprioceptive force measurements for confirmation
Actuation	VIA not stiff or accurate enough	performance limitation, additional feedback, breaks on stop
	actuation not safety certified	laboratory proof of concept and external safety measures
Gesture recognition	difficulty of tracking humans in real environments	• use of markers and specific clothing (colors) • special lighting (e.g., infrared) • additional sensors
	gesture misinterpretation	restricted "vocabulary", operator training
Human interaction	difficulty for the robot to infer human motion	additional modalities, confirmation exchanges
	difficulty for the operator to anticipate robot actions	additional modalities, operator training
Real-time implementation	missing capability hampers safety and renders the system unusable	reduced dynamics (robot or human speed)

Modification of power and force limits

an example of risk critical task …
mitigated by application re-design



1. Eliminate pinch and crush points
2. Reduce robot system inertia or mass
3. Reduce robot system velocity

   2. & 3. will reduce energy transfer in a collision
4. Modify robot posture such that contact surface area is increased
5. Avoid sensitive body areas (head & neck)

\+ Safe control: collision detection & reaction

Bibliography

- A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. on Dependable and Secure Computing*, vol. 1, no. 1, pp. 1-23, 2004
- S. Haddadin et al, "The «DLR Crash Report»: Towards a standard crash-testing protocol for robot safety," - Part I: Results, pp. 272–279; Part II: Discussion, pp. 280-287, *IEEE Int. Conf. on Robotics and Automation*, 2009.
- S. Haddadin et al, "Soft-tissue injuries in robotics: An experimental safety study of stab/puncture and incised wounds," *IEEE Robotics and Automation Mag.*, vol. 18, no. 4, pp. 20-34, 2011
- S. Haddadin et al, "On making robots understand safety: Embedding injury knowledge into control," Int. J. of Robotics Research, vol. 31, no. 13, pp. 1578–1602, 2012
- G. Hirzinger et al, "On a new generation of torque controlled lightweight robots," *IEEE Int. Conf. on Robotics and Automation*, pp. 3356-3363, 2001
- ISO 10218:2011. Robots and robotic devices – Safety requirements for industrial robots, Part 1: Robots, https://www.iso.org/standard/51330.html; Safety requirements for industrial robots, Part 2: Robot systems and integration, https://www.iso.org/standard/41571.html, July 1, 2011
- ISO TS 15066:2016. Robots and robotic devices – Collaborative robots, https://www.iso.org/standard/62996.html, February 15, 2016
- J.K. Salisbury, W. Townsend, B. Eberman, D. DiPietro, "Preliminary design of a whole-arm manipulation system (WAMS)," *IEEE Int. Conf. on Robotics and Automation*, pp. 254-260, 1988
- M. Zinn, O. Khatib, B. Roth, J.K. Salisbury, "Playing it safe: A new actuation concept for human-friendly robot design," *IEEE Robotics and Automation Mag.*, vol. 11, no. 2, pp. 12-21, 2004