Risk Assessment, Collaborative Robots, and Engineered Control-Devices

Your presenter is:
Heinz Knackstedt
C &E Safety Specialist
TÜV Functional Safety Engineer – Machinery
hknackstedt@CEAdvancedTech.com
(937) 434-8830 Office
(937) 545-6494 Cell

A Single Source…A Total Solution
Sensing/Connectivity

Safety

Vision

Motion

Automation

Controls

Robots

A Single Source...A Total Solution
Providing automation solutions since 1978
34 knowledgeable Technical Consultants covering Ohio, Kentucky, Indiana, and Tennessee
Same day shipment on stock items
24 hour product availability and technical support

On-line ordering

Non-warranty repair needs
Product training and awareness through seminars, workshops, lunch & learns and webinars – check out our event schedule at www.cesales.com

A Single Source...A Total Solution
Who we are and what we do

Forty years serving the automation industry

34 Technical Consultants who live near their customers

12 Technical Support Specialists, both in the field & in the office

12 Customer Service Reps, quotes, delivery information, expediting

Large inventory; same day shipping on stock items, 95%+ on time delivery

Order online, via EDI, Credit Card, Fax, or Phone

24 Hour emergency assistance

Lunch & Learns, Seminars, Webinars, and in-depth training classes

Generic Technology or Product application specific

Webinars archived on-line

www.cesales.com 800-228-2790

A Single Source… A Total Solution
Goals for the day

• Review the need for and the background of risk assessment
• Identify the “soft side” of risk reduction and what makes a risk reduction measure effective
• An overview of the major steps of the risk assessment process
• Introduce the concept of collaborative robots, what they are and are not, and their application risk reduction strategies
Employee Safety

• Occupational Health and Safety Act -1970 Public Law 91-596 (OSHA)
  – Act Applies to User (Employer) of a piece of equipment,
  – Not its Manufacturer or System Integrator
    • Subject to Civil Court Tort litigation for machine or integration
  – Federal law
    • Written and passed by Congress
    • Administered by either Federal or State OSHA
  – General Duty Clause 5.a

*Each employer shall furnish to each of his employees, employment and a place of employment, which is free from recognized hazards that are causing or are likely to cause death or serious physical harm*
Risk Assessment
Risk Assessment is the:

- SINGLE MOST IMPORTANT step in providing effective machine and plant safety because it:
  - Identifies the possible hazardous situations encountered while performing a specific task,
  - Determines the level of risk for that task
  - Identifies the requirements of the risk reduction measure(s) which will reduce the risk of that task to an acceptable level
  - Leads to the implementation of the risk reduction measure which achieves acceptable risk
The goal of the Risk Assessment process is to reduce risks to acceptable levels.

The Risk Assessment PROCESS is not completed until acceptable risk is achieved.
Risk Assessment Objectives

• Reduce the rate and severity of injuries
• Increase understanding of the hazards and risks of Plant’s Operations
• Identify risk reduction measures which:
  – Reduce Risk
  – Increase or maintain operational efficiency through correctly specified and designed, risk reduction measures
  – Are compatible with plant operations
  – Will be utilized by affected individuals
  – Assure cost effective, sustainable, solutions
• Install, validate, and maintain the risk reduction measures identified
Risk Assessment

• There is no Federal requirement for a formal Hazard Risk Assessment
  – OSHA only requires that risks be “assessed and reduced”
  But

Inspectors ask for documentation to show that this assessment and reduction has been accomplished

• All new and updated Consensus Safety Standards for machinery, now require a Risk Assessment
• Risks must be identified, understood, estimated, evaluated, and ultimately reduced to an acceptable level
• Develop a Risk Reduction measure, which accurately defines how the risk is to be reduced to an acceptable level, for each hazardous situation,
There is no such thing a “ZERO” risk

Acceptable Risk.

- A risk level achieved after risk reduction measures have been applied. It is a risk level that is accepted for a given task (hazardous situation) or hazard
- The expression “acceptable risk” usually, but not always, refers to the level at which further technologically, functionally, and financially feasible risk reduction measures or additional expenditure of resources will not result in a significant reduction of the risk.
Risk Assessment

Option

• Use a Consultant who provides a Risk Assessment document as a deliverable for a fee
  – Advantages
    • Consultant is an “expert” at hazard identification, risk reduction, and safety standards
    • Requires less plant manpower resources
  – Disadvantage
    • Does not have the operational knowledge of the plant
    • Not familiar with current plant safety issues
    • Tends to provide a Hazard Identification and standard risk reduction solutions which may not be tailored to machine or plant’s operational needs
    • Difficult to update R.A. after a process or machine change
Risk Assessment
Option

• Conduct a risk assessment using an In-Plant team
  – Advantages
    • Heightened awareness of tasks, hazards, and risks
    • Best risk reduction measure is often a machine or process change which could also increase operational performance
    • Group consensus typically provides the best operational solution
    • Increased acceptance of risk reduction measures when developed with input from operations personnel:
      – Most familiar with operational requirements
      – Aware of “undocumented” tasks
    • Data available for other processes/machines or update
  – Disadvantages
    • Requires management commitment to empower team
    • Requires plant manpower resources
The “Soft Side” issues of risk reduction
Risk Assessment

Plant Operations have a major impact on the selection and effectiveness of risk reduction measures.
• There is NO plant which has not recently had an accident!!

• An accident is any UNPLANNED or UNEXPECTED outcome of an event, usually undesirable
  – It does not necessarily result in an injury
  – A near miss is an accident which, if repeated through continued exposure, will ultimately result in an injury

• All of the factors which resulted in a near miss at one exposure to the hazard, might not be present in the same measure to prevent an injury at the next occurrence
  – The majority of injuries are preceded by unresolved close calls or near misses

• There are between 7 to 9 “Close Calls” for every 1 Injury

Required: A Paradigm Shift
FACT!
Poor design is most often the root cause for the circumvention of safeguarding devices and risk reduction measures

“Value” Analysis by the Operator

Perceived Risk and its resultant Reduction

....vs....

Effort to Use the Risk Reduction Measure

• Influences impacting Safety Behavior
  • Perception
    • How dangerous is it now, what is my personal risk?
    • How much is my risk reduced if I use the risk reduction measure?
  • Habit
    • I’ve always done it this way “‘cause that’s the best way”
  • Obstacles
    • The risk reduction measure makes it more difficult to ……..
  • Barriers
    • The risk reduction measure prevents me from ……..

“Understanding Influences on Risks: A Four-Part Model” Terry Mathis, Shawn Galloway ProAct Safety  EHS Today  10 Feb 2010

Without a “Value” the risk reduction measures will not be used

A “GOOD” risk reduction measure addresses these concerns
Use of risk reduction measures and means

• The most effective method of preventing defeating or bypassing of a risk reduction measure is to **remove the incentive to do so**

• Provide special machine operating modes with their own risk reduction features to assure that specific tasks may be carried out safely and easily, without circumvention of risk reduction measures

EX: MIG welder: Provide special manual operating mode for feeding weld wire which removes power from all unnecessary components and other equipment but provides manual control of those required for the job, such as a jog function for the wire feed rolls.

  If torch is mounted on a robot, provide a “dress tip” position at a small opening in the perimeter fence which removes the need for the operator to enter the safeguarded space.
# Incentive to Defeat Safeguards

## Brief Instructions:
1. Add operating modes if appropriate
2. Determine relevant tasks
3. Complete blue cells line by line

### Modes of operation
- Benefits without protective device:
  - 0 None
  - + Minor
  - ++ Substantial

### Tasks:
1. Help
2. Automatic Setup Manual etc.
3. Help Help Help
4. Help
5. Initial Operation Program test/ test run
6. Setup/adjustment conversion/tooling/
7. Machining
8. Manual intervention for swarf removal
9. Manual change of workpiece
10. Manual intervention for trouble shooting
11. Checking/random sampling
12. Manual intervention for measuring/ finetuning
13. Manual change of tools
14. Maintenance/ servicing
15. Rectification of faults

### Incentive to bypass the task:
- Task permissible, e.g. for larger workpieces
- Task possible in these modes without tampering?
- Faster, greater productivity?
- Improved flow of movement etc.
- Greater precision
- More convenient
- Less freedom of movement
- Reduced travel
- Better visibility
- Better audibility

### Avoidance of interruptions for the task:
- Greater use, e.g. for larger workpieces
- Faster, greater productivity
- Improved flow of movement etc.
- Greater precision
- More convenient
- Less freedom of movement
- Reduced travel
- Better visibility
- Better audibility
Cause for Manipulation (Defeating) of Safeguarding Devices and Measures

Result of many of Machine Injuries due to Functional Safety Specification Errors

Fig. 12 Subjectively perceived “necessity” of manipulating protective devices according to operating modes (n = specifications as part of an empirical study; multiple answers possible)

Taken from Best of MRL-News “Safety of Machinery and Machine Control Systems”
Schmersal/Elan publications  Apr 2011
The value of a complete and thorough Risk Assessment
Causes of Process Safety Incidences

Safety Related Parts of the Control System (SRP/CS) did not provide the Required level of Risk Reduction.

85% 65% Already wrong before start of operation. These are Quality issues not Hardware Failures. Systematic errors which must be Reduced by Fault Avoidance through specification and design quality measures and Validation.

ONLY 15% ARE FROM OPERATIONS AND RANDOM FAILURES

Source: “Out of Control” UK Health and Safety Executive (HSE) (September 2004)
Risk Assessment

The Process

An Overview
Risk Assessment - the Process

• Objective is not just to assess risk but to reduce the risk to an acceptable level

• Identify the machine life cycle for the Risk Assessment
  – Design, Build, Install, Commission, Operate, Maintain, De-commission, Dispose

• Determine the use limits of the machine or process
  – Function, Operation, Product, Material

• Identify Tasks
  – Operations located at, on, or near the machine/equipment
  • Include both Production and Repeated/Routine Maintenance
    – For major maintenance projects, do separate risk assessment for those tasks specific to that activity
  – Activities in the area affected by the machine or process
Risk Assessment, the Process
Continued

• Identify Users and their tasks

• Identify Hazards
  – All components and situations which can result in an injury if individuals are exposed

• Task / Hazard Pairs
  – For each specific task, identify all hazards or hazardous situations to which personnel can be exposed during its execution

• For each Task / Hazard pair:
  – Estimate the Risk
    • The level of risk from any one hazard may vary with the task
  – Evaluate the level of risk,
    • Is it acceptable or must it be reduced?
Risk Assessment, the Process
Continued

• For each Task / Hazard pair with unacceptable risk:
  – Identify possible risk reduction measures, and choose the most applicable
  – Verify that the risk reduction measure chosen:
    • Reduces the risk to an acceptable level
    • If Functional Safety, meets the required performance level
  – Repeat process until acceptable residual risk is achieved
Risk Assessment, the Process

Continued

• Develop risk reduction implementation plans and track their progress
• Develop Validation plans of how the actual performance of the implemented risk reduction measures may be tested safely and completely
• Develop and implement training program on correct use of the risk reduction measures
• Document and track performance and utilization of installed risk reduction measures
Risk Assessment Process

1. Prepare for and Set Limits of the Assessment
2. Identify Tasks and Hazards
3. Assess Initial Risk
   Risk Scoring Systems
4. Reduce Risk
   Hazard Control Hierarchy
5. Assess Residual Risk
   Risk Scoring Systems
6. Residual Risk Acceptable?
   Yes
   New or Next Hazard?
   No
   Re-evaluate Task
7. Validate Solutions
8. Results / Documentation

ANSI/B11.0 Figure 6 — The Risk Assessment Process
Risk Assessment
The details
Attitude/Equipment/Components for an IN PLANT Risk Assessment

- **Enthusiastic support from upper management**
  - For Safety
  - For Change
  - For the Risk Assessment process
  - For the implementation, utilization, and maintenance of identified risk reduction solutions

- **Diverse, knowledgeable, and interested team** which can work together to **reach a consensus**

- **Clear team understanding** of any special rules or limits

- **Facilitator** who, has no vested interest in specifics of the outcome, but will manage the Risk Assessment **Process** to assure that:
  - Brain Storming is used to identify possibilities
  - All views are solicited, presented, and fairly evaluated,
  - Consensus is reached to obtain a risk reduction solution

- **Methodology** to evaluate and track risks and risk reduction
  - Optional commercial Risk Assessment Software
Risk Assessment, Estimation

• There are a number of Risk Estimation procedures and rating systems
  – Each seeks to use the variables of:
    • Severity of injury
    • Probability of that harm
  – Together, these identify a relative level of risk
    • Risk = Severity * Probability of harm

• The choice of the risk estimation tool is less important than the process itself.
  – The benefit of Risk Assessment comes from the discipline of the process rather than the absolute accuracy of the results

• Resources are better spent on actual risk reduction rather than attempting to attain absolute precision in the estimation of the risk
Identify the Users and their Tasks

- Operations
  - Automatic, Manual
- Interventions are normally the most dangerous as they may be unpredictable and are frequently unplanned
  - Tooling jams, bad material, broken tools, incorrect set-up, material feeder jams
- Set-up and changeover
- Minor Maintenance and adjustment, lubrication, replacing wear items
- Movement of consumables, productive material, waste material, and finished goods
- Loading process components and supplies
- Trouble shooting the process or machine
- Cleaning
- Foreseeable misuse
- Activity in the vicinity of the machine
  - Truck/Fork Lift traffic with process materials and finished goods
  - Passers by
Identify the Hazards

• For a Risk Assessment on installed equipment, **mentally** remove all risk reduction measures
  – These may be retained as a risk reduction measure, if they meet the requirement, as determined by the Risk Assessment
• Shear, Cut, Crush, Pinch, Entrap, Strike, Puncture, Burn
• Trip, Slip, Fall
• Electric, Pneumatic, and Hydraulic, energy
• Gravity, Radiation, Thermal, Trapped or Residual energy
• Ejected tools or materials
• Ergonomic
  – Lifting, Repetitive motion
• Environmental hazards
  – Smog, Weld Slag, Plating and Washing Waste Water
  – These often change with material being processed, such as hazardous smog while welding galvanized vs mild steel
Identify all hazards or hazardous situations to which individuals can be exposed while performing each task, including foreseeable misuse.

Each is a TASK/HAZARD PAIR.
Estimate the Risk

- Risk is a combination of:
  - Most likely Severity of Injury and
  - Probability of Occurrence of that Harm
    - Frequency and length of exposure to the hazardous situation
    - Ability to avoid the injury
    - Probability of the occurrence of the hazardous situation
- Specialized Skills or Training may **NOT** be used to reduce the risk in the initial estimation of the risk
  - Training may be used to reduce risk **BUT only after the innate risk has been correctly estimated, training identified, and when implemented as a part of the risk reduction measures**
- The risk from a given hazard may vary depending on the exposure during one task versus another
- Standards and many Risk Estimation tools are available which relate task/hazard pairs to their level of risk
Selection Criterion and Guidelines

• Select injury severity which is the **most likely**, not the worst conceivable.
  – The occurrence probability is for that level of severity

• **Exposure due to Frequency or Duration**
  – Based on the assumption that exposure ultimately leads to injury
    • Frequency, how often is an individual exposed to the hazard
    • Duration, how long is the individual exposed to the hazard

• **Probability of Occurrence**
  – History of **accidents** in similar circumstances
    • Near Misses should be viewed as hazardous events
    • Under what conditions will the hazard be present
      – Always, sometimes, seldom, only if something else fails
  – What is the possibility to escape the hazard and avoid the injury
    • Warning, Speed, Clearances,
    • **General** Knowledge of Individual(s)
Examples of Level of Risk Estimation Methodology

<table>
<thead>
<tr>
<th>Or Activity</th>
<th>Likelihood of OCCURRENCE or EXPOSURE for selected Unit of Time or Activity</th>
<th>NEGLIGIBLE</th>
<th>MARGINAL</th>
<th>CRITICAL</th>
<th>CATASTROPHIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>MEDIUM</td>
<td>SERIOUS</td>
<td>HIGH</td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>Probably</td>
<td>MEDIUM</td>
<td>SERIOUS</td>
<td>HIGH</td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>SERIOUS</td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>Remote</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>SERIOUS</td>
<td></td>
</tr>
<tr>
<td>Improbable</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
<td></td>
</tr>
</tbody>
</table>

**Likelihood:**
- **Frequent:** Likely to occur repeatedly
- **Probable:** Likely to occur several times
- **Occasional:** Likely to occur sometime
- **Remote:** Not likely to occur
- **Improbable:** Very unlikely – may assume exposure will not happen

**Severity/Consequence:**
- **Negligible:** First Aid or Minor Medical Treatment
- **Marginal:** Minor injury, lost workday accident
- **Critical:** Disability in excess of 3 months
- **Catastrophic:** Death or permanent total disability

**Risk Level:**
- **LOW:** Risk Acceptable, Remedial Action Discretionary
- **MEDIUM:** Take Remedial action at appropriate time
- **SERIOUS:** High priority remedial action
- **HIGH:** Operation not permissible

**Note:** these definitions are provided for illustrative purposes only, and each organization will need to define these terms for their own risk assessment process.
Example of a Risk Estimation Tool

Risk Assessment for Robots from ANSI/RIA TR R15.306-2016

![Risk Assessment Diagram]

**Table 2 – Risk level decision matrix**

<table>
<thead>
<tr>
<th>Severity of Injury</th>
<th>Exposure to the Hazard</th>
<th>Avoidance of the Hazard</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>E0 - Prevented</td>
<td></td>
<td>A1 - Likely</td>
<td>NEGLIGIBLE</td>
</tr>
<tr>
<td>S1 - Minor</td>
<td>E1 - Low</td>
<td>A2/A3 - Not likely/Not possible</td>
<td>LOW</td>
</tr>
<tr>
<td></td>
<td>E2 - High</td>
<td></td>
<td>MEDIUM</td>
</tr>
<tr>
<td>S2 - Moderate</td>
<td>E1 - Low</td>
<td>A1 - Likely</td>
<td>HIGH</td>
</tr>
<tr>
<td></td>
<td>E2 - High</td>
<td>A2/A3 - Not likely/Not possible</td>
<td>HIGH</td>
</tr>
<tr>
<td></td>
<td>E0 - Prevented</td>
<td></td>
<td>LOW</td>
</tr>
<tr>
<td>S3 - Serious</td>
<td>E1 - Low</td>
<td>A1/A2 - Likely/Not likely</td>
<td>HIGH</td>
</tr>
<tr>
<td></td>
<td>E2 - High</td>
<td>A3 - Not possible</td>
<td>VERY HIGH</td>
</tr>
</tbody>
</table>

Task/Hazard Pair
### Example of terms for Risk Estimation

<table>
<thead>
<tr>
<th>Factor</th>
<th>Rating</th>
<th>Criteria (Examples) – choose most likely</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Injury Severity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serious S3</td>
<td></td>
<td>Normally non-reversible; likely will not return to the same job after recovery from incident:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- fatality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- limb amputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- long term disability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- chronic illness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is SERIOUS</td>
</tr>
<tr>
<td>Moderate S2</td>
<td></td>
<td>Normally reversible; likely will return to the same job after recovery from incident:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- broken bones</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- severe laceration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- short hospitalization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- short term disability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- lost time (multi-day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- fingertip amputation (not thumb)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is MODERATE</td>
</tr>
<tr>
<td>Minor S1</td>
<td></td>
<td>First aid; no recovery required before returning to job:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- bruising</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- small cuts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- no loss time (multi-day)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- does not require attention by a medical doctor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is MINOR</td>
</tr>
<tr>
<td><strong>Exposure</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevented E0</td>
<td></td>
<td>- Exposure to hazard(s) is eliminated/controlled/limited by inherently safe design measures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Use of guards prevents exposure or access to the hazard(s) (see Part 2, 5.10). If an interlocked guard is selected, the following bullet must also be met.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If functional safety is used as a risk reduction measure, the implemented functional safety performance (PL) meets or exceeds the required functional safety performance (PL). See Part 2, 5.2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is PREVENTED</td>
</tr>
<tr>
<td>High E2</td>
<td></td>
<td>- Typically more than once per day or shift</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Frequent or multiple short duration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Situations which could lead to increases in the duration of a task, not to include teaching tasks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is HIGH</td>
</tr>
<tr>
<td>Low E1</td>
<td></td>
<td>- Typically less than or once per day or shift</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Occasional short durations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If either of the above are applicable, the rating is LOW</td>
</tr>
<tr>
<td><strong>Not possible</strong></td>
<td>A3</td>
<td>- Insufficient clearance to move out of the way and safety-rated reduced speed control is not used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The robot system or cell layout causes the operator to be trapped, with the escape route toward the hazard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Safeguarding is not expected to offer protection from the process hazard (e.g. explosion or eruption hazard)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is NOT POSSIBLE</td>
</tr>
<tr>
<td>Not likely A2</td>
<td></td>
<td>- Insufficient clearance to move out of the way and safety-rated reduced speed control is used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Obstructed path to move to safe area</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hazard is moving faster than reduced speed (250 mm/sec)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Inadequate warning/reaction time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The hazard is imperceptible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is NOT LIKELY</td>
</tr>
<tr>
<td>Likely A1</td>
<td></td>
<td>- Sufficient clearance to move out of the way</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hazard is incapable of moving greater than reduced speed (250 mm/sec)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Adequate warning/reaction time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Positioned in a safe location away from the hazard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If any of the above are applicable, the rating is LIKELY</td>
</tr>
</tbody>
</table>

1 E0, E2 and E1 are purposely presented in this order (see 6.4.1.2)
Risk Assessment

Evaluation of the Risk

Is current risk level acceptable?  
“YES”

Potential Administrative measures to further reduce residual risk
Risk Assessment

Is current risk level acceptable?

“NO”

Current Risk Not Acceptable, You must Reduce the Risk

What risk reduction measures or methods will achieve acceptable risk?
Before deciding on a Risk Reduction measure, review the requirement for use of Lock Out /Tag Out (LOTO)
A risk assessment, to determine whether the task can and should be done under LOTO, must precede selection of all risk reduction measures which do not directly reduce the risk to an acceptable level through:

- Hazard elimination or necessary level of risk reduction by design
- Fixed guard which will not be removed to accomplish the task
- An individual is not exposed to a hazard
Lock Out-Tag Out

To provide protection from UNEXPECTED energization, start up, or release of hazardous energy

ANSI/ASSP Z244.1-2016 provides additional guidance on the use and design of Alternative Methods when the Risk Assessment has established that total Lock-Out is not practicable for that task
Risk Mitigation / Reduction

- Risk Reduction Hierarchy
  - List of actions is in descending order of effectiveness at reducing or managing the risk
    1. Elimination by redesign/substitution
    2. Reduction by *irreversible* redesign/substitution
       - Reduce severity of injury
       - Reduce available Force
       - Improve ability to escape
       - Reduce maximum speed
       - Reduce frequency of exposure
       - Change process or location of task
    3. Fixed Guards
    4. Safeguarding Devices
    5. Awareness Devices
       - Active
       - Passive
    6. Training and Procedures
    7. Personal Protective Equipment

Directly impact the hazard

Functional Safety
- Depends on action of personnel to be effective
Functional Safety

• The use of control-devices, logic, and circuit design to prevent exposure to the hazard
  – Control hazard to attain a lower level of risk
    • Sequenced multiple forces or speeds
  – Attain a safe state before hazard can be reached
  – Prevent access to by physical control (lock) until the hazard has reached a safe state

• Functional Safety depends on the proper functioning of components and systems for the risk reduction
  – A Fixed Guard is not Functional Safety
  – An interlocked guard which shuts down the drive of a hazardous machine is Functional Safety

• The failure to danger of a Functional Safety system, increases the risk Back to its initial level
The simple Truth

• If nothing ever failed, any circuit which eliminated the hazard would be acceptable, regardless of the level of risk that the hazard represented

• BUT……………………………!
HOPE is not a safety strategy!
Is that the Back-Bone of your Safety Program?

http://www.txt2pic.com
Risk Level and Functional Safety

• The higher the level of risk, the more reliable the Functional Safety System design must be to prevent the loss of the safety function due a failure to danger of any of its components

• There are only three results of a failure to danger of a safety function component
  – Detection, reaching a safe state, and system repair
  – A close call or near miss accident
  – An Injury accident

• If Functional Safety is to reduce a given risk to an acceptable level
  – It must be designed with the appropriate reliability performance level and withstand component failures with an acceptable result
Correlation of Level of Risk Reduction required, to a Functional Safety System’s Circuit Design

- Some risk assessment tools have a mapping technique to convert level of risk to an appropriate performance level (PL_r) of a functional safety circuit

- Machine safety design standards may contain mapping, which takes variables similar to those identified in the risk assessment, to identify the performance level requirement of the functional safety circuit
Performance Level Risk Reduction Graph for Functional Safety

Adapted from ISO 13849-1-2015

Operation of a population of machines for a period equal to the $MTTF_D$ ($\lambda$) means that 63% of them will have experienced a failure to danger over that time period.

$\lambda = 1/h$

$h$ is Mean Time to Dangerous Failure $MTTF_D$ in hours

One year of $24/7=8760$ hr or just under $10^4$ hours

$< 3.8 \times 10^{-5}$

$< 10^{-5}$

$< 3 \times 10^{-6}$

$< 10^{-6}$

$< 10^{-7}$
Performance Level Risk Reduction Graph for Functional Safety

Key
1 starting point for evaluation of safety function’s contribution to risk reduction
L low contribution to risk reduction
H high contribution to risk reduction
PL_r required performance level

Risk parameters:
S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)
F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P possibility of avoiding hazard or limiting harm
P1 possible under specific conditions
P2 scarcely possible

ISO 13849-1 Annex A Figure A.1
A Map of Level of Risk to Performance level
For Robot Applications only

For Robot Applications only. From RIA TR R15.306-2016

Relationship of the Risk Level to the Required Performance Level (PLr) of the SRP/CS

The SRP/CS performance is based on ISO 13849-1

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>PLr</th>
<th>Structure Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEGLIGIBLE (see 6.5.3.1)</td>
<td>b</td>
<td>-</td>
</tr>
<tr>
<td>LOW</td>
<td>c</td>
<td>2</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>d</td>
<td>2</td>
</tr>
<tr>
<td>HIGH</td>
<td>d</td>
<td>3</td>
</tr>
<tr>
<td>VERY HIGH (see 6.5.3.2)</td>
<td>e</td>
<td>4</td>
</tr>
</tbody>
</table>

SRP/CS requirement for risks meeting NEGLIGIBLE risk level

Table 5 Minimum functional safety performance requirements as function of the risk level ANSI/RIA TR R15.306:2016
Safety Related Part of the Control System

Functional Safety block diagram

- Each circuit has these three elements of either:
  - Individual components
  - Sub-systems of groups of individual devices
  - Encapsulated sub-systems which perform the three functions and may serve as any of the three blocks
- A failure to danger in any block in the series safety block diagram, can lead to the loss of the safety function
  - To evaluate safety performance, each proposed SRP/CS must be broken into a block diagram of Safety Failure Events
  - Note: this includes the interconnection of the blocks
    - Networks, even wires, have their own failure modes
What does the “category’s” structure look like?

Cat B & Cat 1 = Single Channel
Cat B = also often called “Simple”
Single failure to danger leads to the loss of the safety function
Cat 1 uses “Better Stuff”,
“Well Tried Components” with a history of acceptable performance in safety applications, typically with longer Mean Time to DANGEROUS Failure (MTTF\textsubscript{D}), and usually includes some “Safety Rated” devices
What does the “category’s” structure look like?

**Cat 2**

Cat 2 = Single Channel with monitoring for failure to danger

Monitor at “suitable” interval $\sim 100x$

Channel use rate or automatically

Not all designs are able to shut down the hazard, but may only warn and/or inhibit next hazardous cycle/situation
What does the “category’s” structure look like?

Cat 3

Cat 3 = Dual Channel

w/ Conditional Monitoring (May not detect all failures to danger)

Single fault will not cause the loss of the safety function

Multiple undetected faults may cause the loss of the safety function

Safety Block Diagram

Dashed monitoring lines represent reasonably practicable fault detection
What does the “category’s” structure look like?

**Safety Block Diagram**

**Cat 4**

Cat 4 = Dual Channel

w/ Complete Monitoring

Faults to danger of components will not cause the loss of the safety function

Must detect first fault or continue to protect with this and the next fault, this combination must be detected

---

**Solid monitoring lines represent technically feasible fault detection**
Performance Level of Safety Function requirements by Risk Level

**PL**

Cat. B  DC\text{aux} None  Cat. 1  DC\text{aux} None  Cat. 2  DC\text{aux} Low  Cat. 2  DC\text{aux} Medium  Cat. 3  DC\text{aux} Low  Cat. 3  DC\text{aux} Medium  Cat. 4  DC\text{aux} High

**Performance Level (PL)**

- **Negligible**
- **Low**
- **Medium**
- **High**
- **Very High**

**Mean Time to Dangerous Failure of Each Channel (MTTF\text{d})**

- **MTTF\text{d} – Low**: $3 \text{ years} \leq \text{MTTF\text{d}} < 10 \text{ years}$
- **MTTF\text{d} – Medium**: $10 \text{ years} \leq \text{MTTF\text{d}} < 30 \text{ years}$
- **MTTF\text{d} – High**: $30 \text{ years} \leq \text{MTTF\text{d}} < 100 \text{ years}$

**Diagnostic Coverage (DC)**

- **Denotation**: None, Low, Medium, High
- **Range**: DC < 60%, 60% ≤ DC < 90%, 90% ≤ DC < 99%, 99% ≤ DC

**Directions Beyond Minimum Requirements**

- Improvement in Combination of Category Structure & Diagnostic Coverage
- Acceptable Area
Verification

- Re-estimate Task/Hazard pair’s risk with the proposed Risk Reduction Measures assumed to be in place
  - Use the same risk estimation process as before to determine:
    - Does the design or process change result in an acceptable level of risk
    - Do any new hazards or task/hazard pairs, which were introduced by the change, result in acceptable risk
    - Is the Safety Function System’s performance level appropriate for level of risk to be reduced

  → Acceptable Residual Risk **may not be claimed** if the proposed Safety Function does not meet or exceed the minimum performance level requirement for the level of risk as determined by the Risk Assessment

  - Does measure meet Human and Environmental needs
  - Does measure meet operational requirements, is sustainable, and will be used
Engineering Compromise
Or
Does my “risk reduction measure” have a FLAW?

A NEW hazard brought on by the “solution”

“Well, thank God we all made it out in time.
... 'Course, now we’re equally screwed.”
Residual Risk

• With the proposed risk reduction measures implemented, will the level of risk then be acceptable?
  – If No
    • Reduce risk from existing or new task/hazard pair(s) with more effective or additional risk reduction measures by repeating the process
  – If Yes
    • Identify remaining residual risks
    • Further reduce these by developing procedures, operating instructions, and training
Implementation and Validation

• Develop Implementation Plan and time table
• Write Validation Plan for each Safety Function, which contains:
  – Functional tests to be performed
    • Operation of the safety function as specified in the R.A.
    • Induce failure modes
    • Include reasonably foreseeable misuse
  – Safe test procedure for each individual test
  – Correct performance of the safety function control
    • Risk reduction functions as described in Plan
    • Auxiliary equipment achieves safe state as required
• Identify any systematic software and logical errors or omissions
• Document the validation test results
Monitor Safety Performance

• Monitor the Machine and its Risk Reduction Measures for:
  – Accident rate
    • Including close calls and near misses
  – Utilization
  – Ability to maintain
A Risk Assessment Example

• The machine
  – Hand load cylinder tube and bracket onto a fixture with automatic clamps
  – Robotic MIG weld bracket to tube
Identify the Tasks

• Operation/production
  – Weld top mounting bracket on strut reservoir
    • Auto mode
      – Load bracket and strut reservoir tube
    • Manual mode
      – Set-up and changeover
      – Movement or replenishment of process material
      – Replace weld wire, dress weld tip
    – Interventions
      » wire jams, bad material, bad clamp position

• Maintenance
  – Trouble shooting
    » Especially those tasks which may require power to accomplish
<table>
<thead>
<tr>
<th>No</th>
<th>Task Description</th>
<th>Hazards</th>
<th>S</th>
<th>E</th>
<th>A</th>
<th>RL</th>
<th>Before Safeguarding</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Tip change</td>
<td>Struck by Robot</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>HI</td>
<td>Interlock gate with safety key lock to drop servo power to robot</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Tip change</td>
<td>Pinch by end effector</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>HI</td>
<td>Interlock gate with safety key lock to drop servo power to robot</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Tip change</td>
<td>Hot Surface</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>MED</td>
<td>Limit Temp w/ cooling system PPE Thermal Protective Gloves</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Replace Weld Wire</td>
<td>Struck by Robot</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>HI</td>
<td>Interlock gate with safety key lock to drop servo power to robot</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Replace Weld Wire</td>
<td>Pinch by end effector</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>MED</td>
<td>Interlock gate with safety key lock to drop servo power to robot</td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td>Replace Weld Wire</td>
<td>Fall from height</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>MED</td>
<td>Lower spool axis, Provide robot low park position</td>
<td></td>
</tr>
<tr>
<td>2.7</td>
<td>Replace Weld Wire</td>
<td>Back injury</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>MED</td>
<td>Provide robot low park position or hoist Use floor pallet and wire de-reel fixture</td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Load Fixture</td>
<td>Struck by Robot</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>HI</td>
<td>Safety Light Curtain to drop servo power to robot</td>
<td></td>
</tr>
<tr>
<td>3.4</td>
<td>Load Fixture</td>
<td>Trap by end effector</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>HI</td>
<td>Safety Light Curtain to drop servo power to robot</td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>Load Fixture</td>
<td>Trap by Clamp tools</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>LO</td>
<td>Safety Light Curtain to drop power to clamp solenoid valves</td>
<td></td>
</tr>
</tbody>
</table>

**Residual Risk**

- Interlock gate with safety key lock to drop servo power to robot
- Limit Temp w/ cooling system PPE Thermal Protective Gloves
- Lower spool axis, Provide robot low park position
- Provide robot low park position or hoist Use floor pallet and wire de-reel fixture
- Safety Light Curtain to drop servo power to robot
- Safety Light Curtain to drop power to clamp solenoid valves

**Note:** If a task is not accomplished during normal production operations, and is not Routine, Repetitive, and Integral to the use of the equipment for Production it is considered by OSHA to be Maintenance vs. Operator Operational activity. It is still listed here. The risk reduction measure is either NORMAL LOCK-OUT TAG-OUT PROCEDURES or ALTERNATE RISK REDUCTION MEASURE (OSHA sub Part O) if LOTO is not practicable.

Ref: CFR 29 1910.147(a) (2) (i) and (ii) See also ANSI Z244.1 LOTO and Alternate Safeguarding
Overview of collaborative robots

• Data in this presentation is derived from ANSI/RIA TR R15.606 Collaborative Robots
  – A United States adoption of ISO/TS 15066
  – A Technical Specification:
    • Is not a standard but is the preliminary publication of data, which with further refinement and testing, is intended to be included in a published Standard (no TS in USA)
    • Represents industry best practice at the time of publication
    • It carries more weight than a Technical Report (TR) which generally is a further explanation of the intent and application of a published standard, which has no mandatory requirements
    • Uses standards terms such as “shall” to indicate a normative, mandatory requirement, which is typically avoided in a TR
  – Applied in conjunction with ANSI/RIA 15.06 Industrial Robot and Robot Systems- Safety Requirements
Collaborative Robot Application
Collaborative Robots

• Goal of Collaborative systems: Combine the repetitive performance of robots with the individual skills and problem solving ability of individuals, through direct interaction within a defined collaborative workspace
  - Traditionally, individuals have been excluded from the industrial robot system’s maximum/restricted space while the robot is active

• Collaborative workspace: a space within the robot operating space where the robot system may perform a task concurrently with an individual, during a production operation.
  - By definition, a robot does not include an end effector or piece part, both of which are added by the user as part of the robot system

Reference ANSI/RIA TR R15.606
Collaborative Robots

- Implementation of a collaborative robot requires a comprehensive risk assessment of:
  - The tasks of both
    - The individual
    - The robot **SYSTEM**
      - Robot, end effector, workpiece, direct support equipment
  - Environment of the collaborative workspace in which they operate
    - Material handling
    - Secondary operations equipment
    - Non associated machines and equipment
    - Structures
Collaborative Applications

• The out of the box “safe” robot **system** is a myth
  – A robot is “partially completed machinery” which may have physical characteristics and safety-rated controls which make it a viable **candidate** for collaborative application
Collaborative Application

• **It is not only the robot itself** which determines if the application may be collaborative with a reasonable risk
  – *Robot manufacturer can only define the safety performance of the robot, not the conditions under which it will ultimately be used*

• **It is the application**, the entire task of the individual and robot system, manufacturing process, and ancillary equipment, which determine if a collaborative application can be achieved with an acceptable level of risk

• Under the correct application conditions, and with built-in or add-on external safety-rated risk reduction controls and measures, any given robot might be capable of collaborative operation for a specific application
Two types of risk reduction approach for Robotic applications

• Traditional Industrial robot applications
  – Risk reduction measures separate the individual from the active robot
  – No contact or shared workspace with the robot

• Collaborative robot applications consist of:
  – Robot System and individual(s) occupying the same workspace
  – Collaborative workspace which contains
    • Portion of the robot system operating space
    • Direct support equipment, including manual operation
    • Other machines or equipment
    • Physical obstructions
Four types of space may be involved, risk reduction measures for each must be identified in the risk assessment

1. Maximum space which an unrestricted robot system can reach
2. Restricted space
   - Robot system mobility area from which it cannot exit
3. Operating space
   - Where the robot may work autonomously
   - Is **not** part of the collaborative workspace,
   - Risk reduction measures here are traditional / non-collaborative
4. Collaborative workspace
   - Specific part of the operating space
   - Individual(s) may work side-by-side with an operating robot system
   - Collaborative risk reduction measures

**Key**

1. Maximum Workspace
2. Restricted Space Boundary
3. Operating Space
4. Collaborative Workspace

Adapted from ANSI/RIA TR R15.606
Risk reduction Strategies for Collaborative Applications

• Robot and individual(s) may occupy the collaborative workspace at the same time

• Types of operating mode:
  – No contact between a MOVING robot system and an individual
  – Robot system is guided by the individual
  – Concurrent movement of individual and robot system
    • Robot actively avoids moving contact with individual
    OR
    • Anticipate occasional contact events of individual(s) with moving robot system
      – The energy and force available to the robot system is limited to such a value that any reasonably foreseeable contact will not produce pain or injury
Risk Reduction Strategies for Collaborative Applications

- For collaborative robot applications, a risk assessment must be completed during the project development to identify all risks, and risk reduction strategies
  - Particularly those risks due to the close proximity of robot system and individuals
- Elements of risk of a collaborative application
  - Tasks of both individual and robot system
  - Robot system
  - Environment of the collaborative workspace
- Determine if a collaborative robot application with acceptable risk is practicable
Risk reduction Strategies for Collaborative Applications

• Determine how the robot system related risks can be reduced to an acceptable level by implementing a combination of:
  – Robot collaborative operation risk reduction strategies
  – Conventional risk reduction measures

• The risk assessment establishes the task’s capability, and possible limitations, of a practicable collaborative application
  – Operational functions of the task
  – Operational and physical limitations of the robot
    • Including special robot functions, typically safety rated
Definitions as used in ANSI/RIA TR R15.606

- **Safety-rated monitored stop**
  - Stop initiated under “normal” collaborative operating conditions
  - Retains power on each robot drive axis (NFPA Stop Cat 2)
    - Prevents motion by controlling axis motor’s rotating field
  - Performance Level PLd structure Category 3
  - May resume collaborative operation when stop conditions clear

- **Safety-rated monitored protective stop**
  - Stop initiated under “abnormal” collaborative operating conditions, to avoid a hazardous situation
  - Removes power from each robot motor drive axis (NFPA Stop Cat 0,1)
    - Prevents motion by engaging axis brake(s), counter balance, mechanical advantage
  - Performance Level PLd structure Category 3
  - Requires manual reset from outside of collaborative workspace
Risk reduction Strategies for Collaborative Applications

• Four types of collaborative operation
  – First three prevent contact with the operating robot system
  • Safety-rated Monitored Stop
  • Hand Guiding
  • Safety-rated Speed and Separation Monitoring
  • Power and Force Limiting
Safety-Rated Monitored Stop

- Robot operates autonomously within the collaborative workspace when no individual is present
- Robot executes a safety-rated monitored stop at the end of a task, or when an individual enters the collaborative workspace
- Resumes autonomous operation when collaborative workspace is clear of individuals
- If the robot moves while an individual is in the collaborative workspace, a safety-rated monitored protective stop is initiated
  - Requires a manual reset to resume collaborative operation
  - Reset device to located outside of the collaborative workspace
Hand Guiding

- Robot may be operating autonomously in collaborative workspace when no individual is in the workspace.
- Robot executes a safety-rated monitored stop at end of task, before individual enters collaborative workspace.
- Operator hand guides robot arm with safety-rated monitored hand guiding device, with enabling device, to control robot motion.
  - Releasing hand guide, executes a safety-rated monitored stop.
- Robot may resume autonomous operation when collaborative workspace is clear of individuals.
- If individuals enter collaborative workspace when robot is not in safety-rated monitored stop, executes a safety-rated monitored protective stop.
  - Requires a manual reset to enable collaborative operation.
  - Reset device is located outside of the collaborative workspace.
Safety-rated Speed and Separation Monitoring

- Robot and individual(s) may move concurrently in the collaborative workspace
- Operating under a safety-rated monitored speed function, the robot maintains at least a safe separation distance from an individual(s) in the collaborative workspace
  - Separation distance may vary with robot speed
  - Robot speed may vary with separation distance
- Resumes collaborative operation from a Safety-rated monitored stop when safety separation distance is reestablished
- Unless Robot is in safety-rated monitored stop, executes a safety-rated monitored protective stop if individual is within safety separation distance
  - Requires a manual reset to resume collaborative operation
  - Reset device to located outside of the collaborative workspace
Power and Force Limiting

• Robot (often referred to as a COBOT) and individual may move concurrently within the collaborative workspace

• The robot system may come into direct contact with an individual either intentionally or accidentally (the contact event)

• PFL is the only collaborative operation in which physical contact between moving robot and individual may be allowed

• Power and Force is limited, so that robot system’s physical contact with an individual in the collaborative workspace will not result in pain or injury
Power and Force Limiting

• The contact event
  – Quasi-static contact (clamping, crushing, or trapping)
    • Will experience both initial impact and continued pressure
    • Includes contact pressure hazard from structure “behind” the body part under pressure of the robot system
  – Transient (Dynamic), individual’s contact area able to rebound from contact (impact) event
    • Pressure during the first 0.5 seconds of the contact event
      • Impact and rebound may propel individual into other structure
Power and Force Limiting

• Risk assessment must be completed in the design development stage to determine if the application can successfully be made PFL
  – Robot System mass and speed determine energy available at the contact event
    • Sum of Mass of moving robot, end effector, and workpiece
    • Robot operation (arm and workpiece speed (TCP) and travel distance)
  – Pressure exerted on the body part by force available
    • Size of contact area determines pressure developed
      – Shape of end effector, rigid workpiece, and support equipment
        » Ex: edges, sharp corners, or projections
Two types of contact event

Effect of object “behind” body part at point of contact, of what otherwise might be an acceptable contact event.

An object in the rebound path or if the robot continues its path after the transient contact, a second contact event may occur.

Adapted from ANSI/RIA TR R15.806
Power and Force Limiting

– Allowable force/energy limits vary by:
  • Type of contact event
  • Location of contact event on the body
    – Areas on which contact must be avoided
    – Mass of the body part
    – Body characteristics of:
      › Spring constant
      › Damping property
      › Skin thickness
  – Pressure limits for onset of pain
Power and Force Limiting

– Ability to anticipate/predict contact events vary by type of interaction between individual and robot

🌟 • Fully coordinated defined task
  • Intervention on an exception basis
  • Proximity to autonomous operation
    – Accidental contact event, typically initiated by the individual
Risk Assessment Detail for Power and Free application

• Identify all reasonably foreseeable contact events
  – Type of contact for each robot system motion which can result in a contact event
  – Worst case body part area of contact for each contact event

ANSI/RIA TR R15.806 Fig2
Typical Cobot PFL Characteristics

• Force limited
  – Robot Arm

• Low kinetic energy
  – Slow combined speed due to all moving axis
  – Low mass robot arm of moving axis
  – Low Load limit
    • Combined mass of end effector & work piece ≤10kg/22lb
  – Short reach ≤1300mm/51in

• Energy transfer of contact limited by speed and force control
  – Inherently safe design
    • Limiting system maximums by fixed robot design
  – Multiple safety-rated monitored features PLr ≥ PLd Cat 3
    • Stop
    • Programmed Speed and Force (Torque)
    • Force Sensing (Collision Detection, w/wo motion reversal)
    • Space Limiting (restricted space) range of motion
  – Features are typically options, to be specified at initial purchase
Typical Cobot PFL Characteristics

- Passive safe physical design
  - No shear or pinch points
  - Rounded members
    - No sharp corners or projections
  - Minimum blind holes or openings
    - Diameter < 6mm dia.
  - Soft covering or skin
    - Could also be force sensing for contact detection
- Easy to program or guide teach to provide flexibility of application
Cobot Application
Risk Reduction Measures

• Limit force and energy available upon contact event
  – Contact force and resulting pressure
  – Energy transferred during contact event, are function of speed and mass
    • Keep these values below maximum threshold based on:
      – Type of contact event
      – Body area contacted during the event

• Eliminate corners and projections and small areas of contact with:
  – Covers, housings, separating surfaces

• Eliminate discontinuous surfaces
  – EX: Square tooling plate mounted on wrist
Cobot Application
Risk Reduction Measures

• Design task to reduce the probability of a contact event

• Design robot system and collaborative workspace to minimize contact and maximize avoidance
  – Design task to avoid robot path
  – Minimize robot path contact with individual’s work pattern
  – Program robot to avoid sensitive body area using space limiting
Quasi-static
Design guide lines

• Limit force
• Force monitoring with robot travel reverse to limit time under pressure
• Large contact area to reduce pressure
• Provide clearance (20” or more) between robot path and fixed objects to prevent trapping
• Follow Transient contact guidelines to manage initial contact impact
Possible Quasi-static impact force – time graph

- **Force or Pressure**
- **Transient limit for relevant body region**
- **Unacceptable region for force or pressure**
- **Quasi-static limit for relevant body region**
- **Acceptable region for force or pressure**

Sample force or pressure curve

- $F_T, P_T$
  - Maximum actual transient value
- $F_S, P_S$
  - Maximum actual quasi-static value

0.5 sec
### Biomechanical Limits of “Pain Onset Level”

<table>
<thead>
<tr>
<th>Body region</th>
<th>Specific body area</th>
<th>Quasi-static contact</th>
<th>Transient contact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Maximum permissible pressure ( \sigma_p ) N/cm(^2)</td>
<td>Maximum permissible force ( F_p ) N</td>
</tr>
<tr>
<td>Skull and forehead</td>
<td>Middle of forehead</td>
<td>40</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>Temple</td>
<td>40</td>
<td>140</td>
</tr>
<tr>
<td>Face</td>
<td>Masticatory muscle</td>
<td>110</td>
<td>not applicable</td>
</tr>
<tr>
<td>Neck</td>
<td>Neck muscle</td>
<td>140</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td>Seventh neck muscle</td>
<td>210</td>
<td>not applicable</td>
</tr>
<tr>
<td>Back and shoulders</td>
<td>Shoulder joint</td>
<td>160</td>
<td>210</td>
</tr>
<tr>
<td></td>
<td>Fifth lumbar vertebra</td>
<td>210</td>
<td>not applicable</td>
</tr>
<tr>
<td>Chest</td>
<td>Sternum</td>
<td>120</td>
<td>140</td>
</tr>
<tr>
<td></td>
<td>Pectoral muscle</td>
<td>170</td>
<td>not applicable</td>
</tr>
<tr>
<td>Abdomen</td>
<td>Abdominal muscle</td>
<td>140</td>
<td>110</td>
</tr>
<tr>
<td>Pelvis</td>
<td>Pelvic bone</td>
<td>210</td>
<td>180</td>
</tr>
<tr>
<td>Upper arms and elbow joints</td>
<td>Deltoid muscle</td>
<td>190</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td>Humerus</td>
<td>220</td>
<td>not applicable</td>
</tr>
<tr>
<td>Lower arms and wrist joints</td>
<td>Radial bone</td>
<td>190</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Forearm muscle</td>
<td>180</td>
<td>160</td>
</tr>
<tr>
<td></td>
<td>Arm nerve</td>
<td>180</td>
<td>not applicable</td>
</tr>
<tr>
<td>Hands and fingers</td>
<td>Forefinger pad D</td>
<td>300</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Forefinger pad ND</td>
<td>270</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Forefinger end joint D</td>
<td>230</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Forefinger end joint ND</td>
<td>220</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Thener eminence</td>
<td>200</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Palm D</td>
<td>260</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Palm ND</td>
<td>250</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Back of the hand D</td>
<td>200</td>
<td>not applicable</td>
</tr>
<tr>
<td></td>
<td>Back of the hand ND</td>
<td>190</td>
<td>not applicable</td>
</tr>
<tr>
<td>Thighs and knees</td>
<td>Thigh muscle</td>
<td>250</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>Kneecap</td>
<td>220</td>
<td>not applicable</td>
</tr>
<tr>
<td>Lower legs</td>
<td>Middle of shin</td>
<td>220</td>
<td>130</td>
</tr>
<tr>
<td></td>
<td>Calf muscle</td>
<td>210</td>
<td>not applicable</td>
</tr>
</tbody>
</table>

1lb = 4.5 Newton  1in\(^2\) = 6.5 cm\(^2\)  N/cm\(^2\) = 1.5 lb./in\(^2\)

NIST Collaborative Robotics: Measuring Blunt Force Impacts on Humans
Transient Impact
Design guide lines

• Keep mass and speed low
  – Safety-rated maximum speed
• Safety-rated force monitoring
• Keep contact area large
• Avoid sharp corners and projections on other objects onto which the individual might be propelled
• Manage results after impact
  – Distance of system reach and force detection reversal to prevent transient impact from becoming Quasi-static
Transient Impact

- Each body part has a maximum transferred energy limit pain threshold
- Energy transferred is a function of
  - Robot system mass
  - Relative travel speeds and directions of robot and body region
  - Mass and spring constant of the body at the area of contact
  - Size of the contact area

ANSI/RIA TR R15.606

Figure A.2 — Contact model for transient contact
Possible Transient force – time graph

- $F_T, P_T$: Maximum actual transient value
- $F_Q, P_Q$: Maximum actual quasi-static value

Unacceptable region for force or pressure

Transient limit for relevant body region

Quasi-static limit for relevant body region

Time

0.5 sec
## Transient Impact

### Table A.3 — Effective masses and spring constants for the body model

<table>
<thead>
<tr>
<th>Body region</th>
<th>Effective spring constant $K$ (N/mm)</th>
<th>Effective mass $m_i$ (kg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skull and forehead</td>
<td>150</td>
<td>4.4</td>
</tr>
<tr>
<td>Face</td>
<td>75</td>
<td>4.4</td>
</tr>
<tr>
<td>Neck</td>
<td>50</td>
<td>1.2</td>
</tr>
<tr>
<td>Back and shoulders</td>
<td>35</td>
<td>40</td>
</tr>
<tr>
<td>Chest</td>
<td>25</td>
<td>40</td>
</tr>
<tr>
<td>Abdomen</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>Pelvis</td>
<td>25</td>
<td>40</td>
</tr>
<tr>
<td>Upper arms and elbow joints</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>Lower arms and wrist joints</td>
<td>40</td>
<td>2</td>
</tr>
<tr>
<td>Hands and fingers</td>
<td>75</td>
<td>0.6</td>
</tr>
<tr>
<td>Thighs and knees</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Lower legs</td>
<td>60</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Mass values for thighs, knees and lower legs are set to the full body weight, recoil or retract from impact while the operator is standing.

For each body region, the maximum permissible energy transfer can be maximum force or maximum pressure values shown in Table A.2 using $E$.

### Table A.4 — Energy limit values based on the body region model

<table>
<thead>
<tr>
<th>Body region</th>
<th>Maximum transferred energy $E$ (J)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skull and forehead</td>
<td>0.23</td>
</tr>
<tr>
<td>Face</td>
<td>0.11</td>
</tr>
<tr>
<td>Neck</td>
<td>0.84</td>
</tr>
<tr>
<td>Back and shoulders</td>
<td>2.5</td>
</tr>
<tr>
<td>Chest</td>
<td>1.6</td>
</tr>
<tr>
<td>Abdomen</td>
<td>2.4</td>
</tr>
<tr>
<td>Pelvis</td>
<td>2.6</td>
</tr>
<tr>
<td>Upper arms and elbow joints</td>
<td>1.5</td>
</tr>
<tr>
<td>Lower arms and wrist joints</td>
<td>1.3</td>
</tr>
<tr>
<td>Hands and fingers</td>
<td>0.49</td>
</tr>
<tr>
<td>Thighs and knees</td>
<td>1.9</td>
</tr>
<tr>
<td>Lower legs</td>
<td>0.52</td>
</tr>
</tbody>
</table>
Graph of maximum speed of a 1cm$^2$ contact event for a given robot system mass at a specific body part

ANSI/RIA TR R15.606 Figure A.4 Graphical representation of calculated speed limit based on the body model
Validation

• The application must be validated by physical measurement testing to assure that the predicted forces and pressures do not exceed the permissible limits
  – Requires specialized equipment and training
  – Testing must be documented
    • Method and equipment used
    • Test results
Measuring force and pressure

Test method attempts to replicate the performance of the target body part

DGUV –Information FB HM-080 8/2017
Validation of power and force limited collaborative robot applications, requires real time testing based on the risk assessment, using specialized sensors and measurements, of any forces applied to exposed parts of the human body, to assure that they are below maximum levels to prevent pain or injury.
Pressure map for quasi-static test using body specific shore value pad and pressure mapping film
Measuring transient impact
Concept being developed

Robot system effective mass dropped at robot velocity

Microfibre cloth for the correction of small surface contours, thickness ≤0.5mm (optional)

Pressure indicating film

Damping material accord. to fabric e.g. hard rubber Shore A=70

Teflon film, thickness ≤0.05mm (optional)

Spring accord. to body region, e.g. 75 N/mm

Force sensor

Mass of body part

Measuring transient impact
Concept being developed
Collaborative Robot Application Synopsis

<table>
<thead>
<tr>
<th>Collaborative type</th>
<th>Benefit</th>
<th>High Risk Applications?</th>
<th>Low Risk Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety-rated monitored stop</td>
<td>Quicker resumption of operation (power retained)</td>
<td>Yes safeguardsing required</td>
<td>Yes</td>
</tr>
<tr>
<td>Hand-guided</td>
<td>Personal control &amp; responsibility by operator; high variability of programs &amp; quick changes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Speed &amp; Separation Monitoring</td>
<td>Reduced space for application; Immediate resumption of higher speeds</td>
<td>Yes safeguardsing required for intrusion/approach</td>
<td>Yes safeguardsing required for intrusion/approach</td>
</tr>
<tr>
<td>Power &amp; Force Limiting (without protective devices)</td>
<td>Reduced space for application; if easy to program, then personal control by operator</td>
<td>Yes, but LOW speed (might be VERY SLOW)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

References

• ANSI B11.0 Safety of Machinery General Requirements and Risk Assessment
• ANSI B11.19 *Performance Requirements for Risk Reduction Measures: Safeguarding and other Means of Reducing Risk*
• ANSI/RIA 15.06 Industrial Robot and Robot Systems- Safety Requirements
• ANSI/RIA TR R15.306 Risk Assessment
• ANSI/RIA TR R15.406 Safeguarding
• ANSI/RIA TR R15.606 Collaborative Robots
• ANSI/RIA TR R15.706 User Guide
• ANSI/RIA TR R15.806 Testing Methods for Power & Force Limited Collaborative Applications
• ISO 13849-1 Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design
• ANSI/ASSP Z244-1 The Control of Hazardous Energy Lockout, Tagout and Alternative Methods
Questions?

Heinz Knackstedt
Safety Specialist
TÜV Functional Safety Engineer
Machinery
C&E Advanced Technologies
677 Congress Park Drive
Dayton, Ohio USA 45459

Office: (937) 434-8830 x252
Cell: (937) 545-6494
hknackstedt@CEAdvancedTech.com