Robotics and Safety – Can Robots be Safe?

Jon Derickson, PE, CSP, Google
and
John McBain, Agilent Technologies
Robotics and Safety - summary

- What is a robot? Where do you find them?
- How can a robot be “safe”? 
- Considerations when evaluating robot safety – hazards, environment, software, users, etc.
- Some applicable safety standards – a brief look
- The underlying requirement – Risk Assessment
- Two case studies:
  - Laboratory robot (Agilent Technologies)
  - Driverless car (Google)
- Q&A
What is a robot?

1. A machine resembling a human being and able to replicate certain human movements and functions.
You may recognize ...
What is a robot?

2. A machine capable of carrying out a complex series of actions automatically.

spot welder ➔
A few current examples ...
Where are robots found?

• In laboratories:
• In operating rooms:
• In your home:
• On your street:
• Even on Mars:
How can these robots be “safe”? 

By “safe” we mean -

• No operator, client or bystander is harmed
• No product, property or facility is damaged

But at the same time we want -

• Useful work to be done quickly
• Robots easily adjusted and controlled
How about this approach?

The **Three Laws of Robotics** are a set of rules devised by the science fiction author Isaac Asimov.

The Three Laws are:

- A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- A robot must obey the orders given to it by human beings, except where such orders would conflict with the First Law.
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.
OK, so what can we really do?

• Analyze the situation for hazards
• Propose rules (standards) for each case
• Test, evaluate and document the device
• Consider possible failures and consequences
  – “It’s not how it works, it’s how it breaks!”
  – Single-fault conditions, but not double-fault
• **Risk management** – analysis, evaluation and control (more about that later)
Hazards – what, where, who, when

• **hazard** - potential source of harm
• We can identify several types of hazards, but it’s not just the type of hazard that influences how to address it. Other factors include:
  – Where? A robot working in a lab or a robot driving down the street?
  – Who? A robot teaching school children or a robot building products with factory workers?
  – When? A robot working at its assigned task or a robot being maintained by a service person?
One hazard type ... and consequences

<table>
<thead>
<tr>
<th>Type of hazard</th>
<th>Examples of hazard</th>
<th>Origins</th>
<th>Potential consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanical</td>
<td>acceleration, deceleration; angular parts; approach of a moving element to a fixed part; cutting parts; elastic elements; falling objects; gravity; height from the ground; high pressure; instability; kinetic energy; machinery mobility; moving elements; rotating elements; rough, slippery surface; sharp edges; stored energy; vacuum.</td>
<td>• being run over; • being thrown; • crushing; • cutting or severing; • drawing-in or trapping; • entanglement; • friction or abrasion; • impact; • injection; • shearing; • slipping, tripping and falling; • stabbing or puncture; • suffocation.</td>
<td></td>
</tr>
</tbody>
</table>
But wait – there’s more!

<table>
<thead>
<tr>
<th>More types of hazards</th>
<th>Possible examples?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electrical hazards</td>
<td></td>
</tr>
<tr>
<td>Thermal hazards</td>
<td></td>
</tr>
<tr>
<td>Noise hazards</td>
<td></td>
</tr>
<tr>
<td>Vibration hazards</td>
<td></td>
</tr>
<tr>
<td>Radiation hazards</td>
<td></td>
</tr>
<tr>
<td>Material / substance hazards</td>
<td></td>
</tr>
<tr>
<td>Ergonomic hazards</td>
<td></td>
</tr>
<tr>
<td>Environmental hazards</td>
<td></td>
</tr>
<tr>
<td>Combinations of hazards</td>
<td></td>
</tr>
</tbody>
</table>
Thousands of standards exist to address these hazards for different types of:

- Hazards
- Products
- Users
- Environments
- Protections
- and so on ....

Here are a few examples of standards that apply to machines with moving parts (such as robots) or to some parts of them:

Some standards that apply to robots are:

UL 1740, Robots and Robotic Equipment
ISO 10218-1:2011, Robots and robotic devices - Safety requirements for industrial robots
IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems
A few examples of Standards

1. ISO 2972, *Numerical control of machines — Symbols*
2. ISO 4413, *Hydraulic fluid power — General rules relating to systems*
3. ISO 4414, *Pneumatic fluid power — General rules relating to systems*
4. ISO 6385, *Ergonomic principles in the design of work systems*
5. ISO 7000, *Graphical symbols for use on equipment — Index and synopsis*
6. ISO 9355-3, *Ergonomic requirements for the design of displays and control actuators — Part 3: Control actuators*
8. ISO 11689, *Acoustics — Procedure for the comparison of noise-emission data for machinery and equipment*
10. ISO 13850, *Safety of machinery — Emergency stop — Principles for design*
A few more examples of Standards

11. ISO 13851, Safety of machinery — Two-hand control devices — Functional aspects and design principles
12. ISO 13854, Safety of machinery — Minimum gaps to avoid crushing of parts of the human body
13. ISO 13855, Safety of machinery — Positioning of protective equipment with respect to the approach speeds of parts of the human body
14. ISO 13856 (all parts), Safety of machinery — Pressure-sensitive protective devices
15. ISO 13857, Safety of machinery — Safety distances to prevent hazard zones being reached by upper and lower limbs
17. ISO 14119, Safety of machinery — Interlocking devices associated with guards — Principles for design and selection
18. ISO 14120:2002, Safety of machinery — Guards — General requirements for the design and construction of fixed and movable guards
20. ISO 14122 (all parts), Safety of machinery — Permanent means of access to machinery
And a few more examples ....

21. ISO 14122-3, Safety of machinery — Permanent means of access to machinery — Part 3: Stairs, stepladders and guard-rails
22. ISO 14123-1, Safety of machinery — Reduction of risks to health from hazardous substances emitted by machinery — Part 1: Principles and specifications for machinery manufacturers
23. ISO 14163, Acoustics — Guidelines for noise control by silencers
24. ISO 15667, Acoustics — Guidelines for noise control by enclosures and cabins
25. IEC 60079-11, Explosive atmospheres — Part 11: Equipment protection by intrinsic safety “i”
26. IEC 60204 (all parts), Safety of machinery — Electrical equipment of machines
27. IEC 61000-6 (all parts), Electromagnetic compatibility (EMC) — Part 6: Generic standards
28. IEC 61496 (all parts), Safety of machinery — Electro-sensitive protective equipment
29. IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems
30. IEC/TS 62046, Safety of machinery — Application of protective equipment to detect the presence of persons
And yet more examples ....

31. IEC 62061, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems
32. IEC 62079, Preparation of instructions — Structuring, content and presentation
33. IEV 191 see IEC 60050-191, International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service
34. CR 1030-1, Hand-arm vibration — Guidelines for vibration hazards reduction — Part 1: Engineering methods by design of machinery
35. EN 614-1, Safety of machinery — Ergonomic design principles — Part 1: Terminology and general principles
36. EN 1299, Mechanical vibration and shock — Vibration isolation of machines — Information for the application of source isolation
37. EN 12198-1, Safety of machinery — Assessment and reduction of risks arising from radiation emitted by machinery — Part 1: General principles
38. EN 12198-3, Safety of machinery — Assessment and reduction of risks arising from radiation emitted by machinery — Part 3: Reduction of radiation by attenuation or screening
39. EN 13861, Safety of machinery — Guidance for the application of ergonomics standards in the design of machinery
Are we safe yet??

• Did you notice that ISO 12100 was about “Risk assessment and risk reduction”, not risk elimination?
• The answer is that we never can eliminate risk, only reduce it to a “tolerable” level.
• This statement becomes more and more applicable as robots become more autonomous and more integrated into daily life.
• So how do we determine “risk” and reduce it to a “tolerable” level?
• Glad you asked …. Here’s Jon Derickson to explain
HAZARD AND RISK ASSESSMENT
Systems “V” Model

- Identify Hazards
- Analyze Hazards & Assess Risks
- Identify Safety Critical Functions & Controls
- Implement Safety Critical Functions & Controls
- Concept of Operations
  - Requirements and Architecture
- Detailed Design
- Operation and Maintenance
  - System Verification and Validation
  - Integration, Test, and Verification
- Implementation
  - Verification and Validation
- Time
- Project Definition
- Project Test and Integration
- Release for Production
- Safety Validation and Assessment
Safety Approach

Establish Safety Requirements

- Derived Safety Requirements
  - Hazard Analysis
  - Design Reviews
  - Software Req’ts Analysis
  - Concurrent Engineering Specifications
  - Regulatory Req’ts
  - Feedback from Field Data

Develop a Design Approach to Meet the Requirements

- Development Teams
  - Identify design approach and specific requirements

Results

- Good Design (H/W and S/W Specifications)
- Assessment of Residual or “Inherent” hazards
- Test/Verification Requirements
- Cautions/Warnings Training Procedures
- Quality Assurance Requirements
Hazard and Risk Analysis Process

Understand the system

- Intended use
- Reasonably foreseeable misuse
- Operational environments
- Operator interface
- Maintenance
- Testing
- Training
- Shipping
- Storage

Identify Hazards

Evaluate the risks

Develop hazard controls

Implement hazard controls

Verify Implementation
# Example – Risk Assessment Criteria

<table>
<thead>
<tr>
<th>Category</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>I</td>
<td>Event results in death, permanent total disability, loss of assets exceeding $1M, or irreversible severe environment damage that violates law or regulation.</td>
</tr>
<tr>
<td>Critical</td>
<td>II</td>
<td>Event results in permanent partial disability, injuries or occupational illness that may result in hospitalization of &gt; 5 days, loss of assets exceeding $200K but less than $1M, or a reversible environment damage causing a violation of law/regulation.</td>
</tr>
<tr>
<td>Marginal</td>
<td>III</td>
<td>Event results in injury or occupational illness resulting in hospitalization of &lt; 5 days, loss exceeding $40K but less than $200K, or mitigable environment damage without violation of law or regulation where restoration activities can be accomplished.</td>
</tr>
<tr>
<td>Negligible</td>
<td>IV</td>
<td>Event results in injury or illness not resulting in hospitalization of &lt; 1 day, loss exceeding $2K but less than $40K, or minimal environment damage not violating law or regulation.</td>
</tr>
</tbody>
</table>

## Qualitative Description

<table>
<thead>
<tr>
<th>Level</th>
<th>Likelihood</th>
<th>Individual Item</th>
<th>Fleet or Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Frequent</td>
<td>Likely to occur often in the life of an item, with a probability of occurrence greater than $1 \times 10^{-1}$ in that life.</td>
<td>Continuously experienced.</td>
</tr>
<tr>
<td>B</td>
<td>Probable</td>
<td>Will occur several times in the life of an item, with a probability of occurrence less than $1 \times 10^{-1}$ but greater than $1 \times 10^{-2}$ in that life.</td>
<td>Will occur frequently.</td>
</tr>
<tr>
<td>C</td>
<td>Occasional</td>
<td>Likely to occur some time in the life of an item, with a probability of occurrence less than $10^{-2}$ but greater than $1 \times 10^{-3}$ in that life.</td>
<td>Will occur several times.</td>
</tr>
<tr>
<td>D</td>
<td>Remote</td>
<td>Unlikely but possible to occur in the life of an item, with a probability of occurrence less than $10^{-3}$ but greater than $1 \times 10^{-6}$ in that life.</td>
<td>Unlikely, but can reasonably be expected to occur.</td>
</tr>
<tr>
<td>E</td>
<td>Improbable</td>
<td>So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than $1 \times 10^{-6}$ in that life.</td>
<td>Unlikely to occur, but possible.</td>
</tr>
<tr>
<td>F</td>
<td>Extremely Improbable</td>
<td>So improbable, it can be assumed occurrence is impossible probability of occurrence less than $1 \times 10^{-7}$ in item life.</td>
<td>Extremely unlikely to occur, but not impossible.</td>
</tr>
</tbody>
</table>
Example – Risk Management Matrix

<table>
<thead>
<tr>
<th>Hazard Severity</th>
<th>Probability of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frequent (A)</td>
</tr>
<tr>
<td>Catastrophic (I)</td>
<td>High</td>
</tr>
<tr>
<td>Critical (II)</td>
<td>High</td>
</tr>
<tr>
<td>Marginal (III)</td>
<td>Medium</td>
</tr>
<tr>
<td>Negligible (IV)</td>
<td>Low</td>
</tr>
</tbody>
</table>

Hazard Decision Authority Matrix

<table>
<thead>
<tr>
<th>Residual Risk</th>
<th>Integrating Contractor Risk Acceptance</th>
<th>Government Risk Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>Program Director/Senior Leadership</td>
<td>Army Acquisition Executive (AAE)</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Program Manager and Technical Director</td>
<td>Program Executive Officer (PEO)</td>
</tr>
<tr>
<td>LOW</td>
<td>Technical Director</td>
<td>MGV Program Manager (MGV-PM)</td>
</tr>
</tbody>
</table>
Hazard Mitigation Development

Hazard Scenario & Risk Assessment

- Description of hazard concerns
- Effects on people & equipment
- Risk assessment
- Related causes that contribute to hazards
- General design approach for controlling the hazards
- Background Information

Hazard/Cause Mitigations

- Software Behaviors/Constraints
- Hardware Behavior/Constraints
- Interface Constraints
- Warnings and Cautions
- Procedural Controls

Documented in Hazard Log
**Hazard Analysis**

**Hazard Analyses**
- Preliminary Hazard Analysis
- Subsystem Hazard Analyses
- System Hazard Analysis
- Fault Tree Hazard Analysis
- FMEA

**Lessons Learned**
- Component Evaluation
- System Testing
- Reliability testing
- Experiments

**Hazards**
Undesired system behaviors or faults that could lead to serious injury or damage

**Causes**
Logical grouping of cause scenarios that lead to actionable mitigations

**Mitigations**
Specific actionable behaviors or constraints needed to control hazard risk (HW, SW, Procedures)

**Verification**
Results of testing that demonstrates hazard mitigations are effective
Guidelines – Hazard and Cause Development

- Primary objective is to develop meaningful and actionable mitigations to control hazard risk
- Hazards are written as scenarios at a level to which you want to apply risk
  - Scenarios should ideally include elements of energy available to cause harm, the mechanism or conditions that would allow the energy to cause harm and the injury or damage that might result.
- Causes provide more specific details that are intended to lead one logically to specific actionable mitigations.
- The following rules of thumb are helpful in eliminating complexity and duplication
  - Hazards with only one cause may be an opportunity for aggregation with other hazards
  - If several hazards the same causes, you might look for aggregation of the hazards
  - If several causes drive the same mitigations, then you might look for aggregation of the causes
  - If you have more than 10 causes for a hazard, consider breaking it up into multiple hazards
  - If you have more than 10 mitigations for a cause, then you might consider breaking it up
• You have heard about how hazard evaluation and risk assessment can be applied to robots
• Now let’s take a quick look at a couple of case studies
CASE STUDY
LABORATORY
ROBOT
Case study – laboratory robot

Laboratory robot considerations

• What hazards did you notice?
• What methods of protection could you use?
• Are some protection methods acceptable because this robot would be used in a laboratory by trained personnel?
• What hazards could result from single faults?
• How could you protect against those hazards?
• Any other considerations?
Applying Safety to Robots

• The laboratory robot safety is for operating under controlled conditions, so some factors can be discounted.

• Let’s take a look at a robot operating under much less controlled conditions.
Example 2 – Driverless Car

http://www.youtube.com/watch?v=bp9KBrH8H04
What would you need to consider for a driverless car?

• What hazards are possible for its environment?
• What methods of protection could you use?
• Are some protection methods NOT acceptable because this robot would be used in public streets by untrained people?
• What hazards could result from failures?
• How could you protect against those hazards?
• Any other considerations?
And in Conclusion ...

• Robots, like every other product, cannot be 100% safe
• All hazards and hazard mitigations must be considered
• Risk assessment and management will reduce risk to a “tolerable” level
• What is “tolerable” will depend on many factors
QUESTIONS?