CIS 890: High-Assurance Systems

Introduction to Safety Concepts

Lecture: Differences in Conventional Development and Safety-Critical Development

Copyright 2013, John Hatcliff, Kim Fowler. The syllabus and all lectures for this course are copyrighted materials and may not be used in other course settings outside of Kansas State University in their current form or modified form without the express written permission of one of the copyright holders. During this course, students are prohibited from selling notes to or being paid for taking notes by any person or commercial firm without the express written permission of one of the copyright holders.
Objectives

- Understand some of the differences between development of conventional systems and development of safety critical systems
- Understand notion of “process” and how process definitions are often used to guide and constrain development of safety-critical systems
Life-Cycle Processes

- In many contexts, guidelines for achieving a functioning system are phrased in terms of interrelated processes.
- Each process consists of a set of activities (which can be further divided into specific tasks) for achieving desired outcomes.
- Safety-critical system development adds additional processes/activities not found in conventional system development.

Processes and the relationships between them can be visualized in many different ways.
Waterfall Model

Many common process concepts are most easily understood in the “Waterfall Model”

Traditional Waterfall Methodology

1. **Requirements**
2. **Design**
3. **Development**
4. **Testing**
5. **Deployment**
6. **Maintenance**

Capture the intent of the customer and other **stakeholders** in natural language **requirements** statements.

Describe the **architecture** of the system.

Realize the **hardware** and **software** of the system, following the requirements and architecture.

**Verify** that the system realization satisfies the requirements.

Place the system in the **operational context**, **provision/configure** the system to the specifics of the context, and ensure **environment assumptions** made in requirements are satisfied.

**Monitor** the system in operation, **update** hardware and software as necessary to fix problems or improve functionality/features.


In practice, a strict, linearly ordered, implementation of these processes causes issues (e.g., problems are not detected until later stages).
The "V Model"

The V model exposes more of the system architecture decomposition into units, the integration of units into a system, and the relationships between implementation/integration step and corresponding requirements/design steps.

<table>
<thead>
<tr>
<th>Phase 0</th>
<th>Phase 1</th>
<th>Phase 2</th>
<th>Phase 3</th>
<th>Phase 4</th>
<th>Phase 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfacing with Planning and the Regional Architecture</td>
<td>Project Planning and Concept of Operations Development</td>
<td>System Definition and Design</td>
<td>System Development and Implementation</td>
<td>Validation, Operations and Maintenance, Changes &amp; Upgrades</td>
<td>System Retirement / Replacement</td>
</tr>
</tbody>
</table>

Cross-Cutting Activities
- Stakeholder Involvement
- Elicitation
- Project Management Practices
- Risk Management
- Program Metrics
- Configuration Management
- Process Improvement
- Decision Gates
- Trade Studies
- Technical Reviews
- Traceability

Life Cycle Time Line

The Spiral Development Model

Emphasizes development as an iterative activity, with each iteration adding completeness to the final system.
26262 Approach for Process-Oriented Organization of Requirements

Many standards are organized around process specifications.
Elements of a Process Definition

The following illustrates how the details of a process phase may be defined (illustrated for the “Develop System Requirements” process)

Activities within a process

Details of the System Requirements development process

Things that the activities must conform to

Artifacts and previously completed steps that are required by the process

Artifacts that result from completing the process

Constraints
- Project Plan/SEMP
- Configuration Management
- Risk Management

Activities
- Develop requirements
- Write and document requirements
- Check completeness
- Analyze, refine & decompose requirements
- Validate requirements
- Manage requirements

Outputs
- Requirements Specifications
  - System & Sub-systems
- Verification Plan
  - (See Verification Process)

Enablers
- Stakeholder Involvement
- Technical Reviews
- Elicitation
- Trade Studies
- Traceability

http://www.fhwa.dot.gov/cadiv/segb/views/document/sections/section3/3_5_1.cfm
Processes have purposes and desired outcome.

Processes are organized into activities that may proceed sequentially or in parallel.

Each activity may have one or more tasks to perform.
Stakeholders
- Conventional Development

Nowhere more than in the requirements process do the interests of all the stakeholders in a software or system project intersect

- **Customers** -- fund a project or acquire a product to satisfy their organization’s business objectives.
- **Users** -- interact directly or indirectly with the product (a subclass of customers).
- **Requirements analysts** -- write the requirements and communicate them to the development community.
- **Developers** -- design, implement, and maintain the product.
- **Testers** -- determine whether the product behaves as intended.
- **Documentation writers** -- produce user manuals, training materials, and help systems.
Stakeholders
- Conventional Development

Nowhere more than in the requirements process do the interests of all the stakeholders in a software or system project intersect

- **Manufacturing people** – must build the products that contain software.
- **Sales, marketing, field support, help desk, etc.** -- who will have to work with the product and its customers.

*Because requirements are the foundation for both the software development and the project management activities, all stakeholders must be committed to following an effective requirements process.*
Additional Stakeholders in Safety-Critical Systems

Regulatory / Certification Regimes
- FDA
- Federal Aviation Administration

Third-Party Certification Agents
- SAE ARPA4761 Guidelines and Methods
- RTCA DO-178C Summary of Changes
- ISO 14971:2009

Standards

Society at Large

Requirements

Software

Hardware

Product

CIS 890 -- Safety Critical Development
Regulatory Agencies

- Regulatory Agencies
  - may provide *guidance documents* (written within the agency)
  - may *recognize / mandate standards* (developed jointly with industry)

- Standards and Guidance Documents generate additional requirements that manufacturers must consider (beyond simply meeting the needs/desires of the customer)

NRC Regulations
Title 10, Code of Federal Regulations

Requirements binding on all persons and organizations who receive a license from NRC to use nuclear materials or operate nuclear facilities

FDA Guidance Documents

FDA provides many different types of guidance documents to prompt manufacturers to address specific concerns issues. Below are listed a few that are most relevant to our projects...

- **Infusion Pump Guidance**

- **Software Guidance**
  - [http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm](http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm)

- **Use of Off the Shelf Software**

- **Human Factors / User Interfaces**

- **Cyber-Security for Network Enabled Medical Devices**
FDA recognizes (i.e., “officially likes to see the use of”) industry-developed standards. Here are some that are most relevant to our work.

- IEC 60601 -- Medical electrical equipment— Part 1: General requirements for basic safety and essential performance
- ISO 14971 - Medical devices— Application of risk management to medical devices
- ISO 13485 – Medical devices— Quality management systems— Requirements for regulatory purposes
- IEC 80001 - Application of risk management for IT-networks incorporating medical devices
60601 Example of Product Requirement...

4.10.2 Supply mains for ME equipment and ME systems

For ME equipment intended to be connected to supply mains, the following rated voltages shall not be exceeded:

- 250 V for hand-held ME equipment;
- 250 V d.c. or single-phase a.c. or 500 V polyphase a.c. for ME equipment and ME systems with a rated input ≤ 4 kVA; or
- 500 V for all other ME equipment and ME systems.
**4.3 Identification of hazards**

The manufacturer shall compile documentation on known and foreseeable hazards associated with the medical device in both normal and fault conditions.

This documentation shall be maintained in the risk management file.

Compliance is checked by inspection of the risk management file.

*No criteria for evaluating the goodness of this process step!*
5.5.2 Management representative

Top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that includes

a) ensuring that processes needed for the quality management system are established, implemented, and maintained,

b) reporting to top management on the performance of the quality management system and any need for improvement (see 8.5), and

c) ensuring the promotion of awareness of regulatory and customer requirements throughout the organization.
Third-Party Certification

Concept

- Third party certification involves a party other than the manufacturer (first party) and customer/user (second party) that inspects and tests the product against some recognized criteria (e.g., safety, security, interoperability).
- Third party certification organizations provide an increased level of trust in the product.
- Manufacturers can disclose proprietary details to the third party that they would not disclose to competitors or society at large.

Example – Underwriters Laboratories

Benefits
The UL Mark is the most widely recognized and accepted third party certification mark in North America, giving products the surest route to product acceptance by authorities, regulators and vendors. UL uses only full-time qualified engineering staff to complete field evaluations. Because UL is the standards making body for most of the North American product safety standards, field staff have direct access to the Primary Designated Engineers (subject matter experts) and UL Research Engineers when technical support is needed.

Hatcliff et al. FOSE 2014
"[For safety critical systems, typically], the provider-customer cannot settle for a mutual implicit understanding based on implicit information that the system is 'safe enough'. The criticality demands independent assurance (e.g., via third-party certifiers and regulators)."
Adding Safety Requirements

- System Safety Requirements
- Hazard Ranking
- Notions of Loss / Harm
- Hazard Mitigation
- Design away
- Control
- Alert

Software Requirements

Software

Hardware

System

...exists a sequence of events (situation) that can lead to harm

Challenge: Constructing safety requirements requires a number of additional concepts
Good system development involves two major types of “checks/assessments”: verification and validation. Compared to conventional development, both of these concepts have heightened importance in safety-critical systems.
Most deficiencies and disappointments in safety-critical systems occur because the requirements specification does not accurately reflect needs and intent for that system.
Challenge: Safety analysis, system engineering, etc. includes a number of new concepts, techniques, etc. How much of this does a software engineer on a safety-critical system need to know?
The following diagram presents a simplified view of some additional safety assessment steps that get incorporated into the system development process:

- **Design-time hazard analysis** to determine the safety requirements and appropriate design approaches.
- **Post-implementation hazard analysis** to determine that risks are appropriately controlled.

**Figure 1. Traditional “V” Safety Assessment Process in the Avionics Industry**

*Heimdahl “Safety and Software Intensive Systems: Challenges Old and New”*
Integrating Safety Reasoning with Systems Engineering

Leveson’s outline of the system / safety engineering process...

<table>
<thead>
<tr>
<th>Agree on system goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify constraints on how goals can be achieved</td>
</tr>
<tr>
<td>• Define accidents (unacceptable losses)</td>
</tr>
<tr>
<td>• Identify hazards</td>
</tr>
<tr>
<td>• Formulate system-level safety and non-safety constraints</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select a system architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Architectural trade analysis</td>
</tr>
<tr>
<td>• Preliminary hazard analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identify environmental assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a concept of operations</td>
</tr>
<tr>
<td>Perform a preliminary operator task analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Refine goals into testable and achievable system-level functional requirements</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Refine safety constraints and functional requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify preliminary safety control structure</td>
</tr>
<tr>
<td>• Perform STPA</td>
</tr>
</tbody>
</table>

Design-time hazard analysis to determine the safety requirements and appropriate design approaches

*From Leveson “Safer World” – Figure 10.1 (part 1)*
Leveson’s outline of the system / safety engineering process...

<table>
<thead>
<tr>
<th>Safety Engineering Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform safety-driven system design and analysis</td>
</tr>
<tr>
<td>• Make system-level design decisions to satisfy functional requirements and safety constraints</td>
</tr>
<tr>
<td>• Define component responsibilities</td>
</tr>
<tr>
<td>• Identify potentially unsafe control actions and restate as constraints on system and component behavior</td>
</tr>
<tr>
<td>Implementation (construction and manufacturing)</td>
</tr>
<tr>
<td>Document system limitations</td>
</tr>
<tr>
<td>Perform final safety assessment</td>
</tr>
<tr>
<td>Safety certification</td>
</tr>
<tr>
<td>Field testing, installation, and training</td>
</tr>
<tr>
<td>Operations, including maintenance and upgrades</td>
</tr>
<tr>
<td>• Change analysis</td>
</tr>
<tr>
<td>• Incident and accident analysis</td>
</tr>
<tr>
<td>• Performance monitoring</td>
</tr>
<tr>
<td>• Periodic audits</td>
</tr>
<tr>
<td>Decommissioning</td>
</tr>
</tbody>
</table>

Post-implementation hazard analysis to determine that risks are appropriately controlled.

*From Leveson “Safer World” – Figure 10.1 (part 2)*
Hazard Analysis Concepts

Step 1: Identify the potential for inadequate control (improper actuation actions) of the system that could lead to a hazardous state

Example Hazard: Excessive/prolonged heat from Isolette heater harms the infant.
Hazard Analysis Concepts

Step 2: Determine how each potentially hazardous control action identified in Step 1 could occur (identify causes, causal chains)

(Potential Cause 2-1:) Thermostat control algorithm is incorrect (inadequate control algorithm.)

(Potential Cause 2-2:) Current temperature value is incorrect (incorrect feedback)

(Potential Cause 2-2-1:) Temperature sensor has failed (inappropriate operation).

(Potential Cause 2:) Thermostat fails to send “turn off” command (missing control action)

(Potential Cause 1): Failure in Heat Source causes heating element to be constantly on ("turn off" control action not followed).

A control action required for safety is not provided or followed: heater does not turn off even though temperature has reached value/length of duration that is damaging to infant health.

Example Hazard: Excessive/prolonged heat from Isolette heater harms the infant.

This is an example of a “top down” hazard analysis approach. We start from a potential hazard and work backwards through the system to determine faults and errors that could ultimately cause the hazard.
Example Causal Chain

Example Hazard: Excessive/ prolonged heat from Isolette heater harms the infant.

A control action required for safety is not provided or followed: heater does not turn off even though temperature has reached value/ length of duration that is damaging to infant health.

(Potential Cause 2:) Thermostat fails to send “turn off” command (missing control action).

(Potential Cause 2-2:) Current temperature value is incorrect (incorrect feedback).

(Potential Cause 2-2-1:) Temperature sensor has failed (inappropriate operation).

Harm - Excessive/ Prolonged Heat
Applying Results – Use different strategies to mitigate hazards. Note that these mitigations require us to change our system design.

Example Hazard: Excessive/ prolonged heat from Isolette heater harms the infant.

(Potential Cause 2-2-1:) Temperature sensor has failed (inappropriate operation).
(Potential Cause 2-2:) Current temperature value is incorrect (incorrect feedback)
(Potential Cause 2:) Thermostat fails to send “turn off” command (missing control action)

A control action required for safety is not provided or followed: heater does not turn off even though temperature has reached value/ length of duration that is damaging to infant health

Mitigation: provide one or more redundant temperature sensors in the control loop

Mitigation: provide a redundant temperature sensor with a separate alarm system for excessive heat/ cool. The alarm system aims to remove the target of the hazard (infant) from the environment by notifying the clinician to remove infant from Isolette.
Summary of Concepts

Figure 1: Certification Concepts
Identifying Common Faults/Errors

After design is complete, we often do a “bottom up” hazard analysis – we systematically consider each component within the design and ask ourselves “which could go wrong if this component fails?”

Communication
- Late Delivery
- Early Delivery

Value Source (Sensor)
- Detectable Value Error (e.g., Out of Range)
- Undetectable Value Error

Computation (e.g., App) Hosting
- Failure to execute
- Execution delayed
- Interference between computation
Identifying Common Faults / Errors

As an example, IEC 80001-1 has a short list of issues. We anticipate that a significantly expanded list will be necessary to support our work.

1) Loss of function (compromised availability)
   a) Major loss of function
      i) Loss of data (loss of connectivity)
         1) Intermittent connectivity
         2) Complete loss of connectivity
      ii) Loss of function of MEDICAL DEVICE
         1) Incorrect data (compromised integrity)
         2) Incorrect data (PATIENT mismatch)
   b) Degraded function
      i) Incorrect or inappropriate timing of data
      ii) Incorrect or inappropriate data interchange or INTEROPERABILITY
      iii) Unintended interactions between endpoints
      iv) Degraded function of MEDICAL DEVICE

2) Loss of confidentiality
   a) Unauthorized access to data
One source of inspiration is the SAE Standard Error Model Annex for the Architecture Analysis Definition Language (AADL). The AADL Error Modeling framework provides pre-declared hierarchies of error types which can subsequently be refined in an object-oriented fashion (e.g., General refined to Particular).
Emphasis on Assurance

CIS 890 -- Safety Critical Development