Role of the systems engineer in safety critical systems

Dr. Cecilia Haskins, CSEP
Keynote address WOCS
27. September 2012
Roadmap

- About safety critical systems
- Relevant standards, including
- About systems engineering
- Contributions of the systems engineer
- About INCOSE
Therac-25

- The **Therac-25** was a radiation therapy machine.
- It was involved in at least six accidents between 1985 and 1987, in which patients were given massive overdoses of radiation, approximately 100 times the intended dose.

These accidents highlighted the dangers of software control of safety-critical systems, and they have become a standard case study in health informatics and software engineering.
Safety-critical systems

- Safety-critical systems are characterized by:
  - A risk of serious damage to the environment or loss of life – for example, systems used in the control room of a power plant
  - Complex tasks performed by expert users – for example, systems used in surgery
  - Operator control over equipment or people – for example, air traffic control systems
  - Tasks performed under time pressure – for example, in emergency response
Typical domains in which safety-critical systems occur are process control, (for example, nuclear power plants), transportation (for example, air traffic control, railway signalling, intelligent transport systems), medical applications (for example, diagnostic and treatment devices in operating theatres) and emergency management (operations rooms).
Safety-critical systems

• Systems engineers address the specificities of Safety-Critical Design by:
  – Studying the socio-technical context of the system
  – Analysing the cognitive aspects and information needs of complex tasks (cognitive task analysis, link analysis)
  – Eliciting and designing a (shared) mental model to support distributed cognition
  – Developing patterns of interaction that enhance situational awareness
  – Aiming to increase the resilience of the system as a whole
  – Performing a risk analysis to determine which risks can be tolerated, mitigated, eliminated or transferred
The action-retroaction loop in a safety critical system

Both safety critical and high consequence systems have human operators, and increasingly their role is mediated by computer technology. Clearly, in this domain, usability problems can have potentially disastrous consequences.
Issues in safety-critical systems

- What is usability in a safety critical context and how to evaluate it
- How to analyse and reduce the impact of human error through system specification and implementation
- What are possible models of human error that can improve our understanding of them
- How to guarantee the safety of the possible interactions
- How to design for robust co-operation among the users in technologically mediated work
Summarizing the issues

• Interactive safety-critical systems can be characterized by a number of factors:
  – highly trained expert users;
  – the need to react to externally generated events;
  – user control of other physical equipment that is often capable of causing injury to humans;
  – actions are often irreversible and cannot be undone.

• Consequently, there is a strong need to improve awareness of safety issues from the requirement elicitation phase and throughout the product lifecycle.
Automotive safety

The goal of modern automotive systems is to make the average driver as skilled as a professional driver in stabilizing the car under special driving conditions.
Automotive safety

- Modern automobiles can contain 50 – 100 embedded microcontrollers and between 100 MB and 1 GB of object code. Over 85% of a vehicle’s functions are under software control.
- Functional safety is the discipline of ensuring that these systems operate correctly in response to their inputs and thereby maintain safe operation of the vehicle.
- These processes are described in an international standard, “ISO 26262 Road vehicles — Functional safety” which has been developed to address these challenges.
ISO 26262 – automotive safety

safety lifecycle according to ISO including phases for Concept Phase and Product Development
V-model lifecycle approach
Lifecycle approach

- **IEC 61508** is the standard governing the functional safety of programmable electronic systems.
- IEC = International Electrotechnical Commission.
- IEC is well established in the industrial process-control and automation industry and is also influential in automotive, heavy machinery, mining, and other fields where safety and reliability are critical.
- The standard presents a **lifecycle approach** including risk assessment, design, integration, testing, modification and maintenance and safety management.
The IEC EN 61508 standard

The IEC 61508 standard defines the software requirements and sets the safety lifecycle for software, including validation and verification. The safety lifecycle begins with a risk analysis to determine the Safety Integrity Level (SIL) required. SIL is a quantification of the magnitude of risk reduction required.

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Probability of Dangerous Failure Per Hour</th>
<th>Risk Reduction Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>$\geq 10^5$ to $&lt; 10^4$</td>
<td>100,000 to 10,000</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$\geq 10^4$ to $&lt; 10^3$</td>
<td>10,000 to 1,000</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$\geq 10^3$ to $&lt; 10^2$</td>
<td>1,000 to 100</td>
</tr>
<tr>
<td>SIL 1</td>
<td>$\geq 10^2$ to $&lt; 10^1$</td>
<td>100 to 10</td>
</tr>
</tbody>
</table>
Lifecycle analysis of failures causing malfunctions in software-intensive-systems

HSE survey
System Lifecycle Processes Overview per ISO/IEC 15288:2008
Three levels of complexity

- **Level 1**: A sub-system, substantially within one engineering discipline and one organisation. Examples include a PC motherboard, a car gearbox, a sand filter for water treatment, air conditioning, the antenna for an aircraft radio.

- **Level 2**: A system that involves two or more engineering disciplines and/or requires two or more organisations to design, build, operate or maintain it. Examples include an electricity power station, railway signalling, a car, a waste water treatment plant, a hotel.

- **Level 3**: A system of systems that impacts, or is impacted by, many disciplines and economic, social or environmental factors. Examples include the national rail and roads network, the telephone network and electricity supply.

Extracted from ‘Creating systems that work: A publication of the Royal Academy of Engineering 2007.’
Systems Engineering: as defined by INCOSE

- Systems engineering is an interdisciplinary approach and means to enable the realization of successful systems.
- It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, performance, test, manufacturing, cost & schedule, training & support, and disposal.
Systems Engineering: solutions to complex problems

- Systems Engineering integrates all the necessary disciplines and specialty groups into a team effort forming a structured development process that proceeds from concept to production to operation.
- Systems Engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs.
Six principles for integrated system design

- Integrated system design encompasses a wide range of disciplines, skills and ideas.
- The six principles provide a pervasive framework for understanding the challenges of a system design problem and for educating engineers to rise to those challenges:
  1. Debate, define, revise and pursue the purpose
  2. Think holistically
  3. Follow a systematic procedure
  4. Be creative
  5. Take account of the people
  6. Manage the project and the relationships.

Extracted from 'Creating systems that work: A publication of the Royal Academy of Engineering 2007.'
Role of the systems engineer in problem solving situations

- Comprehension - understanding
- Communication – translator services
- Coordination – harmonious functioning
- Cooperation – work toward a goal
- Collaboration – stakeholders, partners
- Continuity – over system life cycle
Focus on enablement

- Comprehension enables with learning
- Communication enables
- Continuity enables over time
- Collaboration enables
- Cooperation enables
- Coordination enables

Systems Engineering enables over time
INCOSE

The International Council on Systems Engineering (INCOSE) is a not-for-profit membership organization founded to advance the art and practice of systems engineering by helping individuals and enterprises turn complexity into competitive advantage.

The Council is committed to shaping a future where systems approaches are preferred and valued in solving problems, whether providing solutions for product development or enabling holistic solutions to global challenges.
INCOSE Mission

Share, promote and advance the best of systems engineering from across the globe for the benefit of humanity and the planet.
Goals

• To provide a focal point for the dissemination of systems engineering knowledge
• To promote international collaboration in systems engineering practice, education, and research
• To assure the establishment of competitive, scalable professional standards in the practice of systems engineering
• To improve the professional status of all persons engaged in the practice of systems engineering
• To encourage governmental and industrial support for research and educational programs that will improve the systems engineering process and its practice
Publications

- *INSIGHT*, quarterly newsletter since 1994
- *Systems Engineering*: peer-reviewed Journal since 1998, 4 issues per year
- *Journal of Enterprise Transformation* – peer-reviewed journal with IIE since 2011
- Conference Proceedings since 1993
- eNote, periodic email notifications
Products

• Products from Working Groups
  – Free to the public on the Web (www.incose.org)
    • Tools Database
    • Technical resource center
  – From the Members Area on INCOSE Connect
    • Measurement Primer
    • Systems Engineering Handbook
    • Systems Engineering Technical Vision 2020
    • Webinar archives
• Products and publications available for purchase through INCOSE Store
Certification

• In 2004 INCOSE initiated the Certified Systems Engineering Professional (CSEP) program; ASEP and CSEP-ACQ (2008); ESEP (2009)

• Certification is open to everyone interested in being recognized formally for their knowledge of systems engineering

• INCOSE members receive reduced rates for initial certification and renewal
Certification options

Multi-Level Base Credentials
The base ASEP, CSEP, and ESEP credentials cover the breadth of systems engineering at increasing levels of leadership, accomplishments, and experience.

Extensions
Extensions cover a specific domain or subset of systems engineering in more detail. A base SEP credential must first be earned.
International Symposia

- 2013 Philadelphia USA
  24-27 June

- 2014 Seoul Korea

- All papers since 1993 available online
Benefits of Membership

- Network with 8000+ systems engineering professionals
- Subscriptions to publications
- Access to all INCOSE products and resources online
- Discounted prices for all INCOSE events and publications
The INCOSE value proposition

• INCOSE
  7670 Opportunity Road, Suite 220
  San Diego, CA 92111-2222
  +1-858-541-1725
  info@incose.org