Chapter 1: Safety-Critical Computer System Design and Evaluation

Howard University Department of Electrical and Computer Engineering
EECE 692 System Safety
Isaac Collins
1.1 The Safety-Critical Computer System

- “Safety-Critical” applies to wide family of applications

- Failure can lead to:
  - Injury
  - Death
  - Property/Environmental Damage
1.1 The Safety-Critical Computer System

- Reasons for Broad Applications:
  - Global Perspective
    - Most safety-related systems don’t fall into high-visibility category
  - **Combined losses of these systems far exceed those that command widespread public attention**
    - In terms of total human suffering and loss of property
1.1 The Safety-Critical Computer System: The Computer System

- In this system, the computer provides real-time control/monitoring of an application
  - Chemical process
  - Aircraft in flight
  - Automobile anti-skid brake
  - Artificial heart
  - Production assembly line

- Application also referred to as “plant” or “process”
1.1 The Computer System, cont’d

- Sensors (Field Instruments)
  - Let computer know what is happening in application
- Effectors (Actuators/Final Elements)
  - Allow computer to control physical parameters in application based on sensed information
1.1 The Computer System, cont’d

- **The Computer**
  - Single-chip microcontroller
  - Custom microprocessor-based controller
  - PLC (Programmable logic controller)
  - DCS (Distributed control system)
  - Airborne flight computer
  - PC-based controller
  - Other programmable electronic systems

- **The Operator**
1.1 The Computer System: Two Basic System Types

- **Computer Control Systems**
  - Operator, computer, sensor, effectors are employed to actively control the application
  - Continuous monitoring, continuously issuing controls

- **Computer Safety Systems**
  - Same components but used to passively monitor the application
  - Continuous monitoring, controls issued when dangerous state is sensed
1.2 Safety-Critical Computer System Design - Overview

- Partitioning the Design Problem:
  - Functional/Operational requirements not directly safety-related
  - Safety-related requirement
    - System does not fail and produce an unsafe condition
1.2 Safety-Critical Computer System Design: Example

- **Industrial Gas Furnace**
  - First (non-safety) Requirement?
    - Automatically control gas flow to maintain temperature
  - Second (safety-related) Requirement?
    - System shouldn’t fail
    - Should not produce an over-temperature condition
1.2 Safety-Critical Computer System Design: Safety Requirements

- **System Safety**
  - Employs distinct set of engineering/management principles, criteria, techniques
  - Help define safety requirements
  - Show how the design process should be structured to realize safe system

- **Key Elements**
  - Addresses the system life cycle
  - Requires a distinct management effort
  - Is a multidisciplinary effort
  - Is built around safety standards
1.2 Safety-Critical Computer System Design: Safety Requirements

- **System Life Cycle**
  - All phases of system’s life
    - Design
    - Research
    - Development
    - Test and Evaluation
    - Production
    - Deployment (inventory)
    - Operations and Support
    - Disposal
1.2 Safety-Critical Computer System Design: Safety Requirements

- **System Safety Management**
  - System may change hands (management) many times
    - Normal Employee Turnover
  - Effective Management Will Include
    - Design and documentation standards and practices
    - System configuration management
    - Tracking system for verifying safety issues raised are resolved
1.2 Safety-Critical Computer System Design: Safety Requirements

• Multidisciplinary Effort
  ▫ Systems are made safe through efforts of all responsible: involved in creation, operation, maintenance, and retirement from service
  ▫ Includes
    • HW/SW design engineers
    • Test engineers
    • Reliability and risk analysts
    • Operating Engineers
    • Maintenance Engineers/Technicians
    • Managers
1.2 Safety-Critical Computer System Design: Safety Requirements

- System Safety
  - Governed by Safety Standards
    - Public Law/Government Regulations
    - Documents produced through work by industry committees, professional societies, safety-related institutions
  - Two Important/Common Standards
    - MIL-STD-882D (Military Standard)
    - IEC 61508 (Commercial Standard)
1.2 Safety-Critical Computer System Design: Safety Requirements

- **MIL-STD-882D**
  - “Standard Practice for System Safety”
  - Issued by DoD in February 2000
  - Presents basic requirements that apply to computer control systems and computer safety systems
  - Contains both *requirements* and *guidance* to aid user in applying standard
  - *Over 300 pages?*
1.2 Safety-Critical Computer System Design: Safety Requirements

- IEC 61508
  - “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems”
  - Approved by International Electrotechnical Commission (IEC) in 2000
  - Several hundred pages
  - Addresses safety-critical computer control systems and computer safety systems
  - Chapter 6...
1.2 Safety-Critical Computer System Design: Mishaps and Mishap Risk

• Mishap
  ▫ An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to environment (MIL-STD-882D)
    • Airliner crash
    • Nuclear meltdown
    • Refinery fire
    • Toxic gas release
    • Natural gas explosion
1.2 Safety-Critical Computer System Design: Mishaps and Mishap Risk

- Mishap Risk
  - An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence (MIL-STD-882D)
    - Possibility of automobile accident
      - Think about not only severity, but also likelihood that the severity could happen
1.2 Safety-Critical Computer System Design: Mishaps and Mishap Risk

- Acceptable Risk?
  - MIL-STD-882D has Four Categories:
    - Negligible
    - Marginal
    - Critical
    - Catastrophic
  
  - Each level assigned based on degree of
    - Human suffering
    - Amount of dollar loss
    - Extent of damage to the environment
1.2 Safety-Critical Computer System Design: Mishaps and Mishap Risk

- Acceptable Risk for IEC 61508?

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Consequence of Safety-Related System Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Minor property and production protection.</td>
</tr>
<tr>
<td>2</td>
<td>Minor property and production protection. Possible employee injury.</td>
</tr>
<tr>
<td>3</td>
<td>Employee and community protection.</td>
</tr>
<tr>
<td>4</td>
<td>Catastrophic community impact.</td>
</tr>
</tbody>
</table>

- Safety Integrity
  - The probability of a system satisfactorily performing safety functions under all stated conditions within stated period of time.
1.3 The Design Process: Hazards

- **Hazard**
  - *Any real or potential condition that can cause*
    - Injury, illness, death to personnel
    - Damage to/loss of system, equipment, or property
    - Damage to environment
  - **Examples**
    - Loss of flight control
    - Loss of nuclear reactor cooling
    - Use of flammable substances
    - Presence of toxic gases in populated environment
    - Presence of natural gas
1.3 The Design Process: Safety-Critical Computer System Design Approach

- **Safety-Critical Approach**
  - Identify hazards and mitigate them so acceptable level of mishap risk is achieved

- **Design Steps**
  - System definition
  - Hazard identification and analysis
  - Mishap risk mitigation
  - Mishap risk assessment and acceptance
1.3 The Design Process: Hazard Identification and Analysis

- After system is defined, identify hazards
  - Based on systematic examination of sources of energy and toxicity in application
    - (formal process beyond the scope of this book)
- Once identified, causes must be determined before design proceeds
  - Fault Tree Analysis (Chpt. 5)
  - Failure Modes and Effects Analysis (Chpt. 5)
1.3 The Design Process: Hazard Identification and Analysis

- **Failure vs Fault**
  - Failure: does not perform a duty or expected action
  - Fault: a defect
- **Example: Effector Failure**
  - System employs computer-actuated safety valve that closes if computer senses a hazardous event
  - Event occurs, computer senses and signals valve
  - Valve may experience *failure* (may not close) due to *fault* of worn bearing (hardware fault), missing spring (personnel error), or excessive ambient temperature (environmental condition)
1.3 The Design Process: Hazard Identification and Analysis

- Mishap Analysis for the Basic System with no safety features
1.3 The Design Process: Mishap Risk Mitigation

- MISHAP
  - INCORPORATE EXTERNAL SAFETY DEVICES
    - HAZARD EVENT (APPLICATION)
      - INCORPORATE INTERNAL SAFETY AND WARNING DEVICES
        - SENSOR FAILURE
        - EFFECTOR FAILURE
        - COMPUTER HARDWARE FAILURE
        - COMPUTER SOFTWARE FAILURE
        - OPERATOR FAILURE
  - IMPROVE RELIABILITY AND QUALITY
    - ONE OR MORE OF:
      - HARDWARE FAULTS
      - SOFTWARE FAULTS
      - PERSONNEL ERROR
      - ENVIRONMENTAL CONDITIONS
      - DESIGN INADEQUACIES
      - PROCEDURAL DEFICIENCIES
      - OTHER CAUSES
1.3 The Design Process: Mishap Risk Mitigation

• Incorporate Internal/External Safety Devices
  ▫ Internal: placed within the computer system
    • Software patches, additional sensors
  ▫ External: placed outside computer system
    • Change of location, personnel, management

• Layers of Protection
  ▫ Distribute effort across all three risk mitigation measures in balanced manner
    • Produces minimum mishap risk
Review

- 1.1 The Safety-Critical Computer System
- 1.2 Safety-Critical Computer Design
- 1.3 The Design Process