EECE 499/693: Computers and Safety Critical Systems

1 Safety-Critical Computer System Design and Evaluation -- Overview

Instructor: Dr. Charles Kim

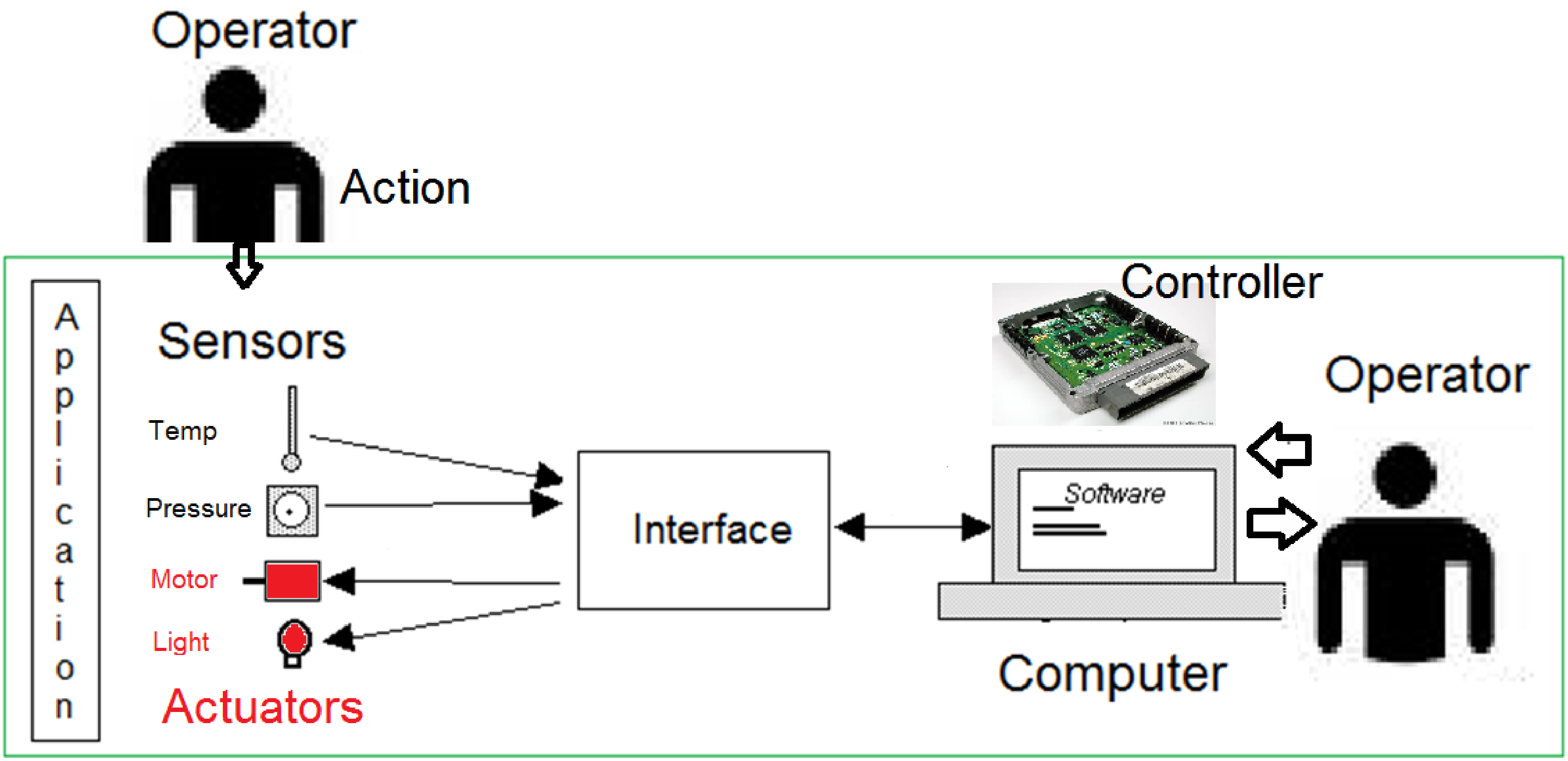
Electrical and Computer Engineering
Howard University

www.mwftr.com/CS2.html

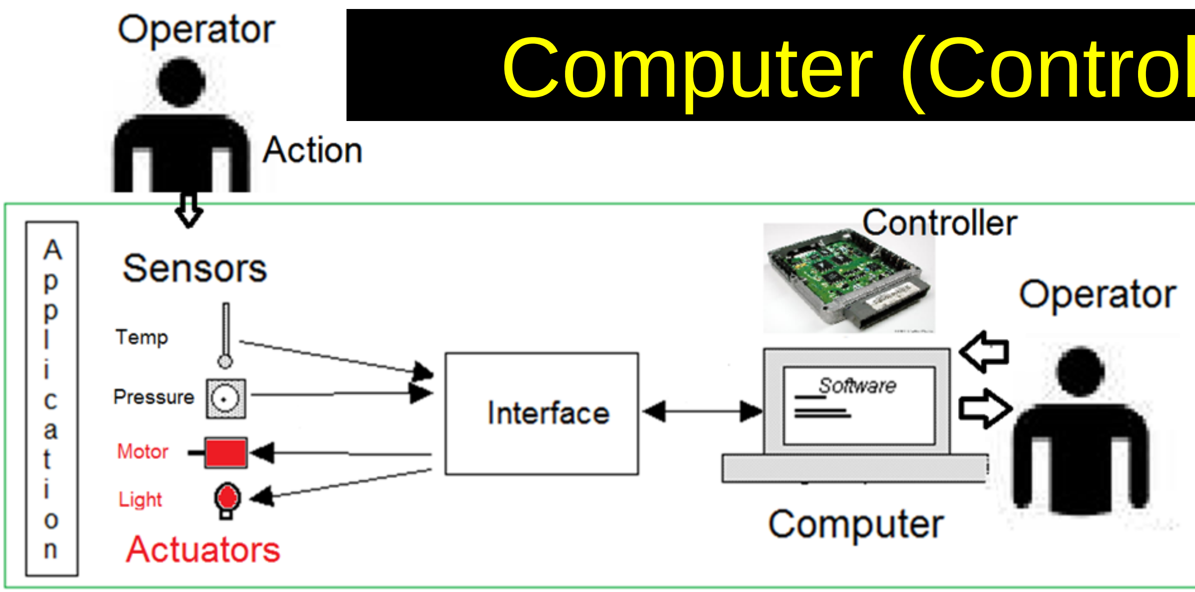
Safety-Critical Computer System

- "Safety-Critical Computer System" applies to wide family of applications
  - Failure can lead to injury, death, property and environmental damage
  - Airliners
  - Small manufacturing facilities

Computer Control System



Computer (Control) System



- **Computer provides real-time control or monitoring of an application ("plant, process"):**
  - Chemical process
  - Aircraft in flight
  - Automobile anti-skid brake
  - Artificial heart
  - Production assembly line
- Computer communicates with application through sensors ("field instrumentation") and effectors ("actuators")
  - Sensors: let the computer know what is going on in the application
  - Effectors: allow the computer to control the physical parameters in the application based on the sensed information
- Operator – human(s) overseeing and managing the function of the overall system **AND/OR** providing input action ("sensor" input) to the system

Sensors and Actuators of Cars--- Example

Computer Control Systems vs. Computer Safety Systems

- 1 Computer Control System:
  - Usual computer control system employed to actively control a safety-critical application by continuously monitoring and issuing controls
- 2 Computer Safety Systems
  - Same or similar computer system which passively monitors a safety-critical application
  - The system is continuously <u>monitored</u> but controls are issued <u>only when the application enters a dangerous state</u>
- The design and evaluation method applies to both of the systems

Safety-Critical Computer System **Design - Overview**

- 1 Design Requirements
  - A set of requirements to control or monitor an application
  - Generally divided into 2 parts
    - A set of functional and operational requirements that are not directly safety-related
    - A set of safety-related requirement that the system not fail and produce an unsafe condition
  - Example in an industrial gas furnace
    - Functional/operational requirement: control gas flow from operator input to maintain temperature profile
    - Safety requirement: the system should not fail and produce an over-temperature condition **(See next slide)**

Example – Collision Avoidance System

- Functional/Operational Requirements
- Safety Requirements

Example --- Unintended Acceleration

- Change in control to avoid UA

Safety-Critical Computer System **Design - Overview**

- 2 Safety Requirements
  - System Safety
    - Not a simple matter of meeting written specifications
    - Instead, design effort to make a system safe
    - It requires a coordinated activities, called "system safety"
    - System safety involves **4 key elements**:
      - **Addresses the system life cycle**: design, research, development, test, evaluation, production, deployment, operations, and disposal
      - **Requires a distinct system management effort**: tracking for verifying all safety issues are resolved amid personnel changes and safety-related changes
      - **Multidisciplinary effort**: hardware and software engineers, reliability and risk analysts, test engineers and technicians
      - **Compliance to safety standards**: MIL-STD-882D (military), IEC 61508 (Commercial)

MIL-STD-882D

- MIL-STD-882D
  - “Standard Practice for System Safety”
  - Issued by DoD in February 2000
  - Original version: MIL-STD-882A in 1960s (for aerospace applications)
  - Presents basic requirements that apply to computer control systems and computer safety systems
  - Contains both requirements (must be followed)and guidance (to aid user in applying standard)
  - Intends to be supplemented with appropriate industry standards in establishing an overall system safety program

IEC 61508

- IEC 61508
  - "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems"
  - Approved by International Electrotechnical Commission (IEC) in 2000
  - Addresses safety-critical computer control systems and computer safety systems
  - Defines functional safety as**:** "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE [*Electrical/ Electronic/Programmable Electronic*] safety-related systems, other technology safety-related systems and external risk reduction facilities."

Concepts of Mishaps and Mishap Risk

- Mishap ("Accident")
  - 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; Train Derailment; Oil Spill.
- 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
- Acceptable Risk
  - MIL-STD-882D has Four Categories:
    - Negligible
    - Marginal
    - Critical
    - Catastrophic

HAZARD RISK ASSESSMENT MATRIX

Frequency of Occurrence	Hazard Categories 1 Catastrophic	2 Critical	3 Serious	4 Minor
(A) Frequent	1A	2A	3A	4A
(B) Probable	1B	2B	3B	4B
(C) Occasional	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

Unacceptable High Medium Low

- Probability Expression - EXAMPLE
    - Computer Control System: "The catastrophic system mishap rate shall not exceed 1.13×10^{-n} per operational hour."
    - Computer Safety System: "he catastrophic system mishap rate shall not exceed 1.13×10^{-n} per demand."

IEC 61508 SIL and Risk

- Safety Integrity ←→ Risk (MIL-STD-882D)
  - Definition: The probability of a system satisfactorily performing the required safety functions under all stated conditions within stated period of time
- IEC 61508 Safety Integrity Levels (SIL)

Safety Integrity Level	Consequence of Safety-Related System Failure
1	Minor property and production protection.
2	Minor property and production protection. Possible employee injury.
3	Employee and community protection.
4	Catastrophic community impact.

- IEC 61508 Sample Quantitative Requirements ←→ Risk Probability

	Computer Control System	Computer Safety System
Safety Integrity Level	Continuous/high-demand mode of operation (probability of dangerous failure per hour)	Low demand mode of operation (probability of failure to perform its safety functions on demand)
1	$\geq 10^{-6}$ to $< 10^{-5}$	$\geq 10^{-2}$ to $< 10^{-1}$
2	$\geq 10^{-7}$ to $< 10^{-6}$	$\geq 10^{-3}$ to $< 10^{-2}$
3	$\geq 10^{-8}$ to $< 10^{-7}$	$\geq 10^{-4}$ to $< 10^{-3}$
4	$\geq 10^{-9}$ to $< 10^{-8}$	$\geq 10^{-5}$ to $< 10^{-4}$

Design Process by Standard

- Overall Design Approach
  - Design Problem : The design problem is that the computer control and computer safety system might fail to perform correctly with the result that a mishap occur.
  - Design Objective: The design objective is to reduce the risk of such mishaps to an acceptable level.
  - Design Approach: Based on MIL-STD-882D by beginning the discussion on mishaps back to their origins --- Causes.

Mishaps vs Hazards

- Design concern is with mishaps
- A mishap ("accident") occurs because of the existence of more than 1 hazards
- A hazard is defined as "any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment"

Mishaps vs. Hazards

www.answers.com/Q/What_is_the_difference_between_a_accident_and_a_hazard

in **THE DIFFERENCE BETWEEN**

What is the difference between a accident and a hazard?

Matthew Albert

Answered Last

The difference between accident and hazard are:
A person is not pre-warned about an accident. It is an unexpected or unforeseen event.

But a hazard is known well in advance. For instance, if I have a culture of Ebola virus in my lab, I know that if by mistake it is released into the environment, me and many others will be in potential danger. So i take precautions to store it in proper conditions.

To be precise, I know that a hazard is a possible source of danger Source(s): Another thing: I can hazard a guess, but i can't accident a guess...

Cloe <333

- Car accident in icy condition

Hazards

- Example of Hazards (→ and Mishaps)
  - Loss of flight control → (____________)
  - Loos of nuclear reactor coolant → (_______)
  - Use of flammable substances → (_______)
  - Train passing through populated area carrying toxic liquid → (_______________)
  - Presence of natural gas → (_________)
- Hazard Identification: The basic approach of designing a safety-critical computer system is to identify hazards and to mitigate them so that an acceptable level of mishap risk is achieved.

Design Steps for Safety

- System definition
- Hazard identification and analysis
- Mishap risk mitigation
- Mishap risk assessment and acceptance

Design Step 1: System Definition

- For General System
  - Define the physical and functional characteristics of the system
  - Understand people, procedures, facilities, and environment that will be involved
- For Computer System
  - Define and understand the application
  - Define the details of the computer system
  - Define operator functions
  - Include system hardware and software
  - Write software requirements – a structured definition for what will be programmed, step-by-step, into hardware.

Software Requirement Spec - Brief

Types of Requirements

- Functional requirements
- Non functional requirements
  - Performance requirements
  - Interface requirements
  - Design constraints
  - Other requirements

Performance Requirements

- Capacity
  - no. of simultaneous users, processing requirements for normal and peak loads, static storage capacity, spare capacity
- Response time
- System priorities for users and functions
- System efficiency
- Availability
- Fault recovery

Functional Requirements

- Transformations (inputs, processing, outputs)
- Requirements for sequencing and parallelism (dynamic requirements)
- Data
  - Inputs and Outputs
  - Stored data
  - Transient data
- Exception handling
- Nature of function: Mandatory/ Desirable/ Optional / Volatile / Stable

External Interface Requirements

- User interfaces
  - eg. if display terminal used, specify required screen formats, menus, report layouts, function keys
- Hardware interfaces
  - characteristics of the interface between the SW product and HW components of the system
- Software interfaces
  - specify the use of other SW products eg. OS, DBMS, other SW packages

- Source: Richards/Dublin

System Definition – Complex Example

- Can we make a “system definition” for the entire automotive electronic systems?

System Definition Example Case – Class Activity

- Select a system and do the "system definition" with emphasis on (1) Functional Requirements and (2) External Interface Requirements of Software Requirement Specification.
  - ABS; Electronic Accelerator; Doors and Seat-belts with Instrumentation; Airbag; Collision Avoidance System; Auto-Parking

System Identification (Software Requirement Spec) Exercise - FORMAT

System Identification Exercise   Name (@ ID)

[with emphasis on Software Requirement Specification:

Note Title   9/9/2014

① Functional Requirements
② External Interface Requirement] ← "sub-title"

System (Application): Collision Avoidance System (EX)

① Functional Requirement

② External Interface Requirement

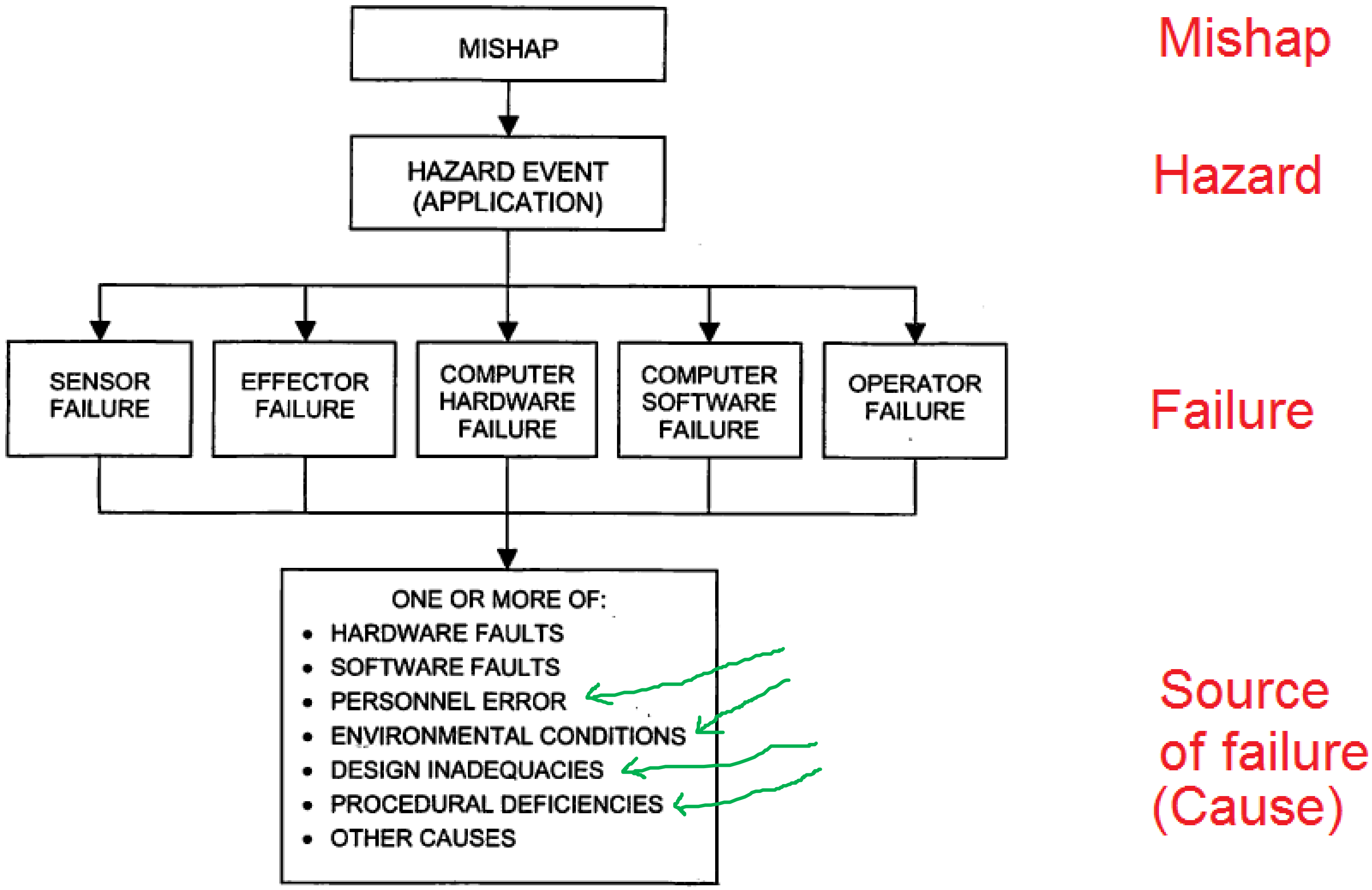
Another Tip for Writing

- "A figure is worth a thousand words;" but without words it collapses.
- Figures are for aiding the words and description; **therefore, description itself should deliver the message. Use figures only when your description alone cannot accurately deliver the message.**

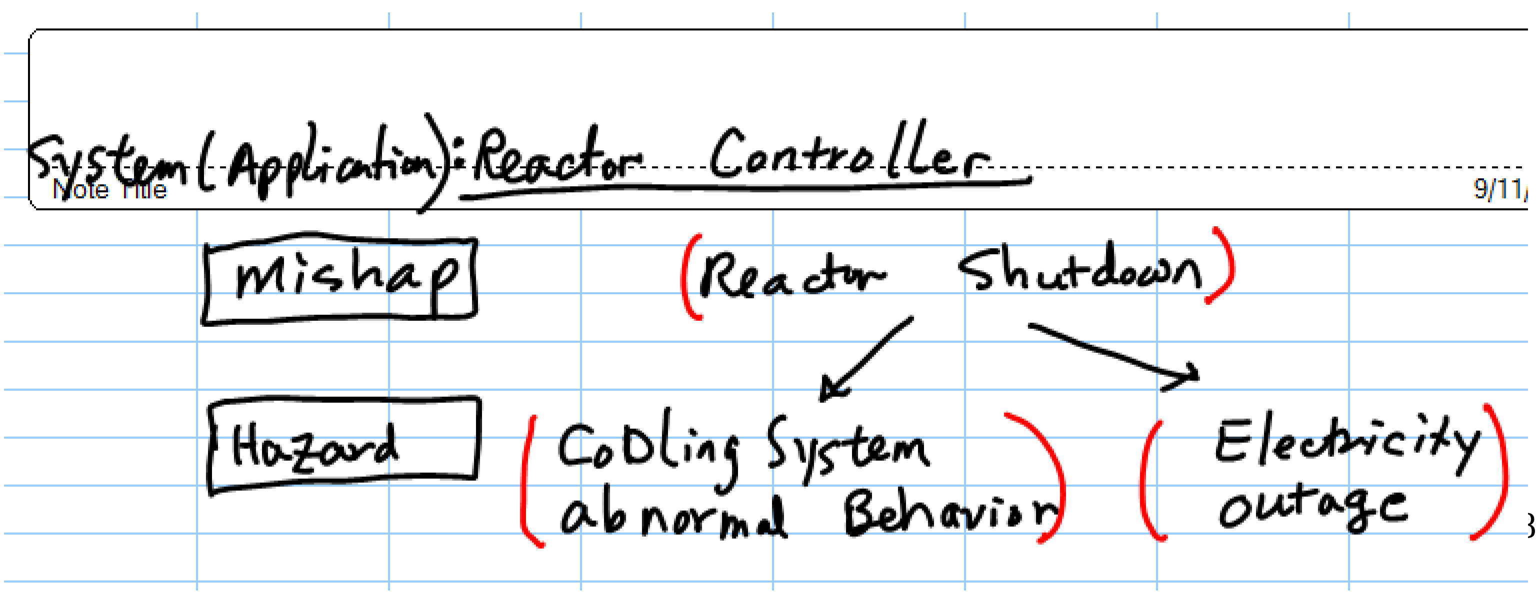
Design Step 2: Hazard Identification and Analysis

- General
  - Identify the hazards associated with the mishaps and determine their causes
  - Use widely know approaches: FTA (fault tree analysis) and FMEA (Failure Modes and Effects Analysis) --- Chapter 5
- Computer Systems
  - Our concern: Hazardous events occur within the application and the system will fail to control it → a mishap ("accident") occurs as a result of failure to control a hazard
  - Mishap Tracking: mishaps are traced to its causes
  - Mishap → Hazard → component failure →sources that cause the failure
  - There are multiple Hazards which may cause a mishap

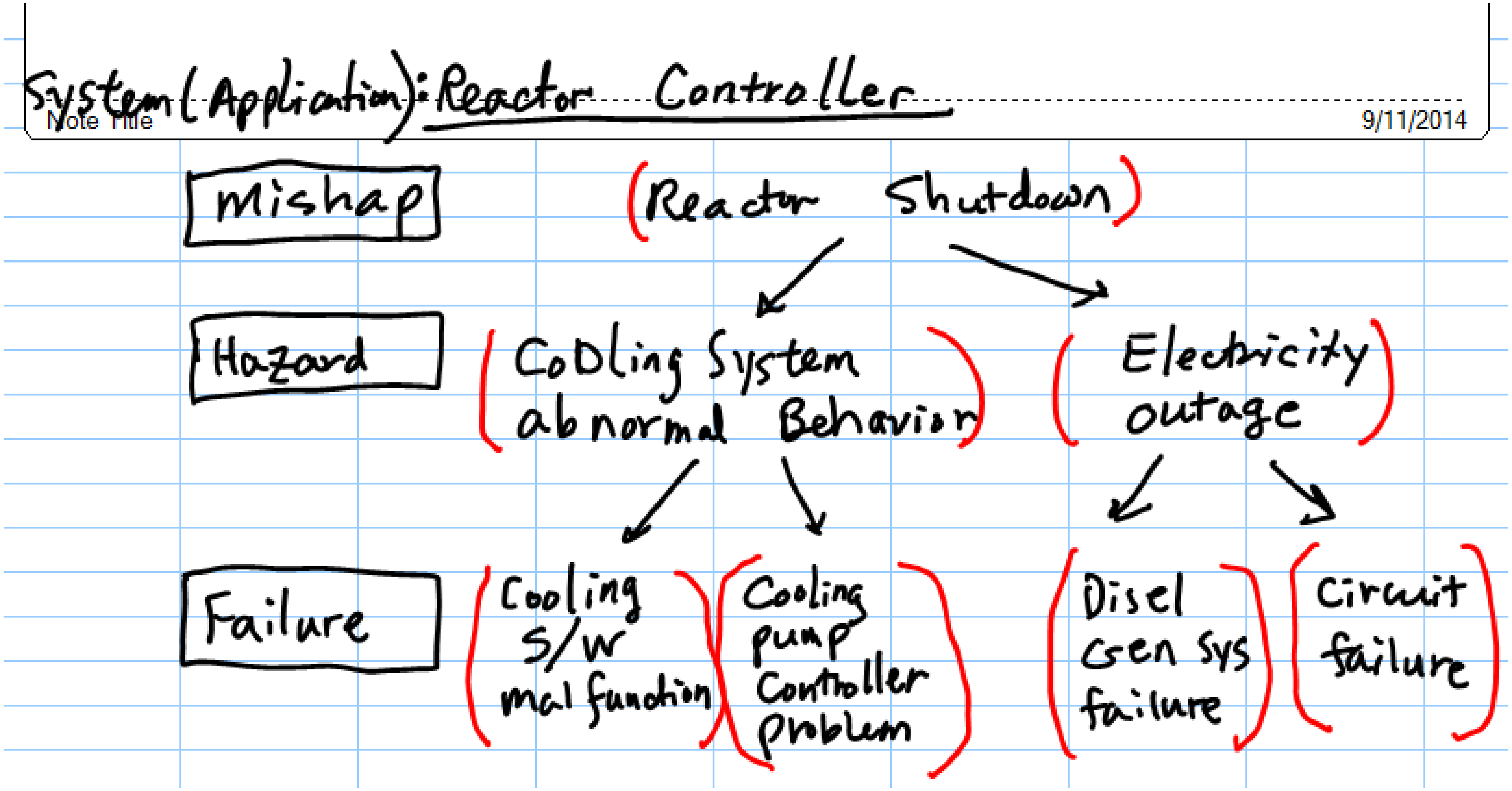
Simple (single) Hazard Analysis Chart



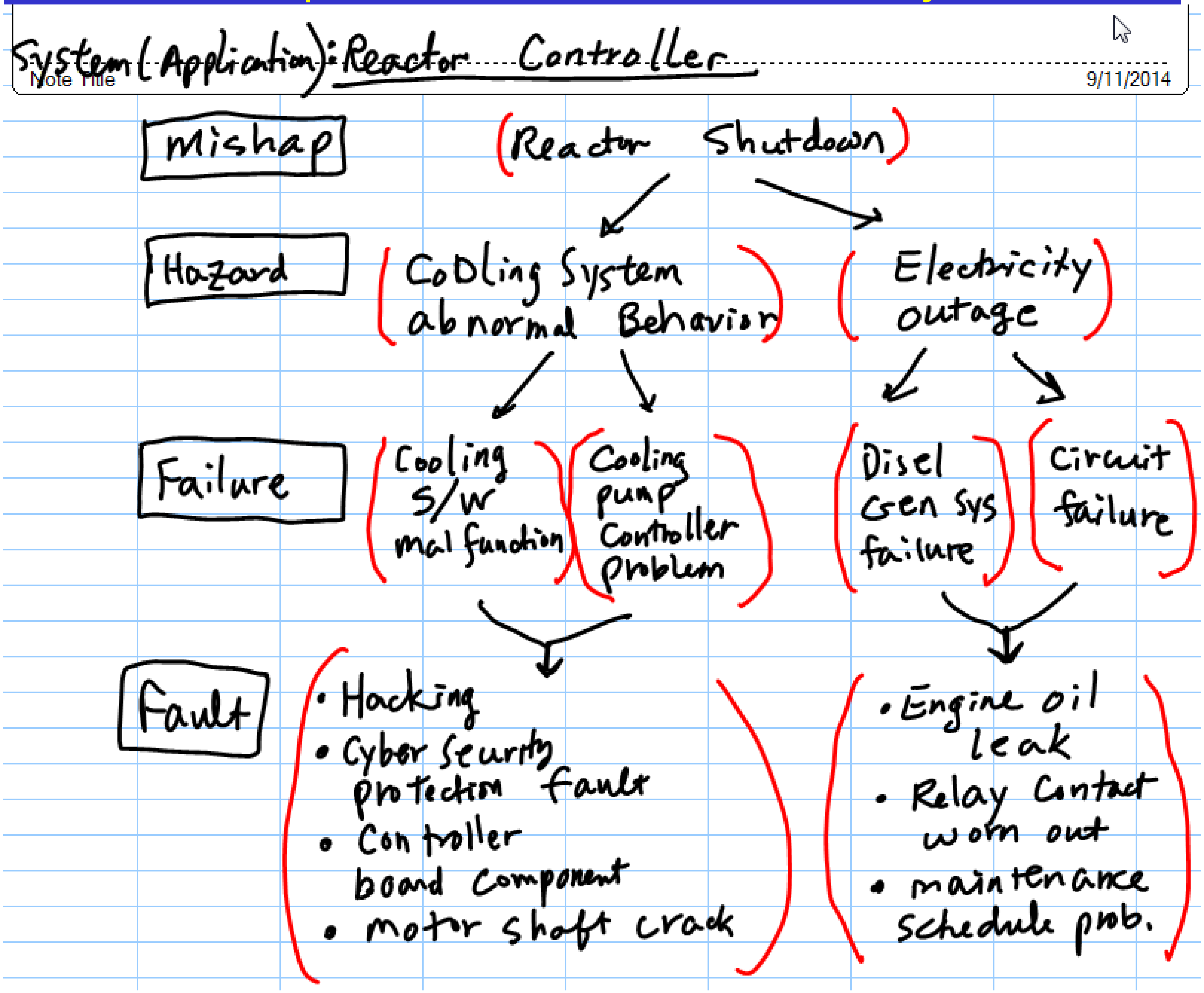
Example Hazard Identification/Analysis



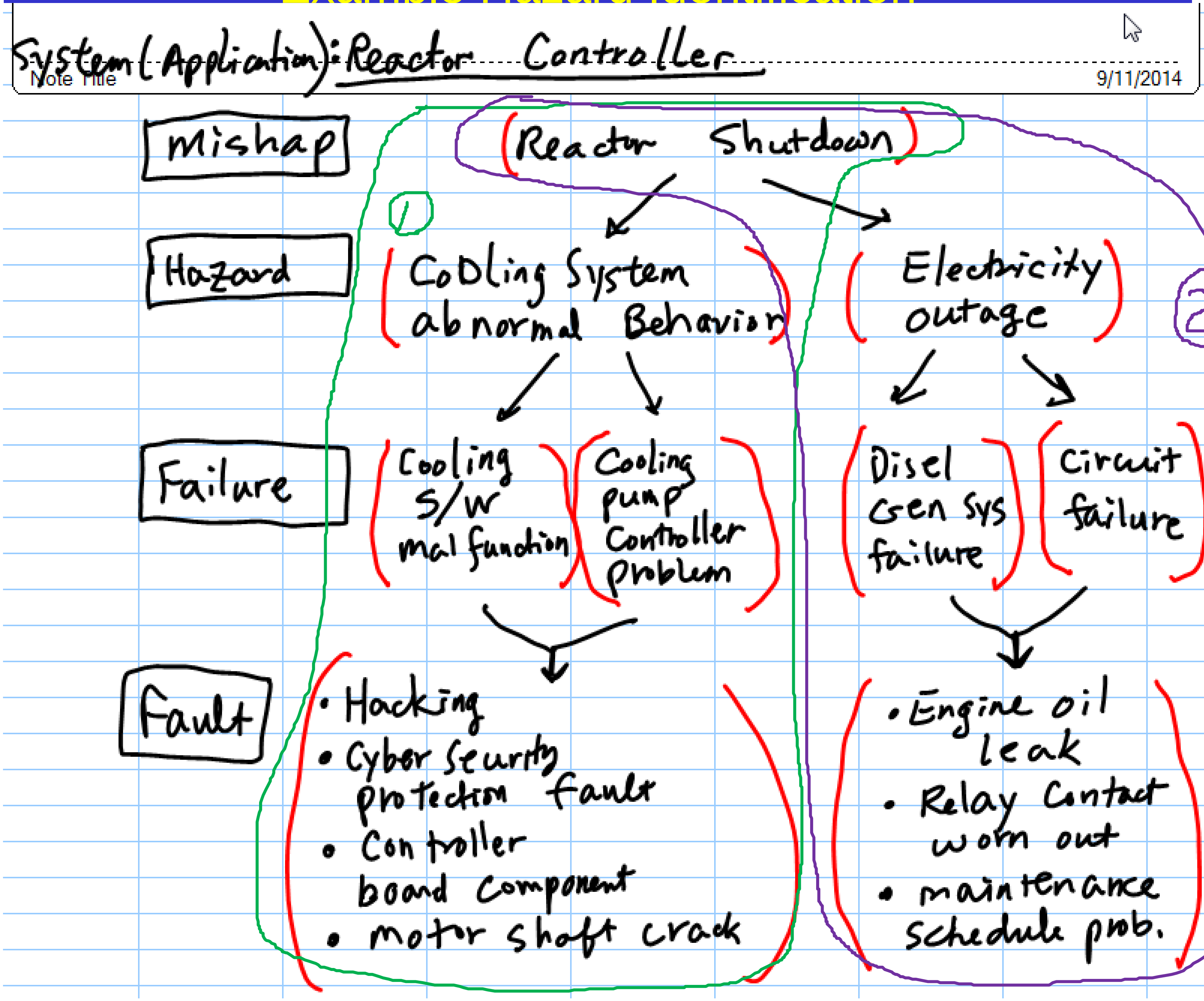
Example Hazard Identification/Analysis



Example Hazard Identification/Analysis



Example Hazard Identification



Failure vs Fault

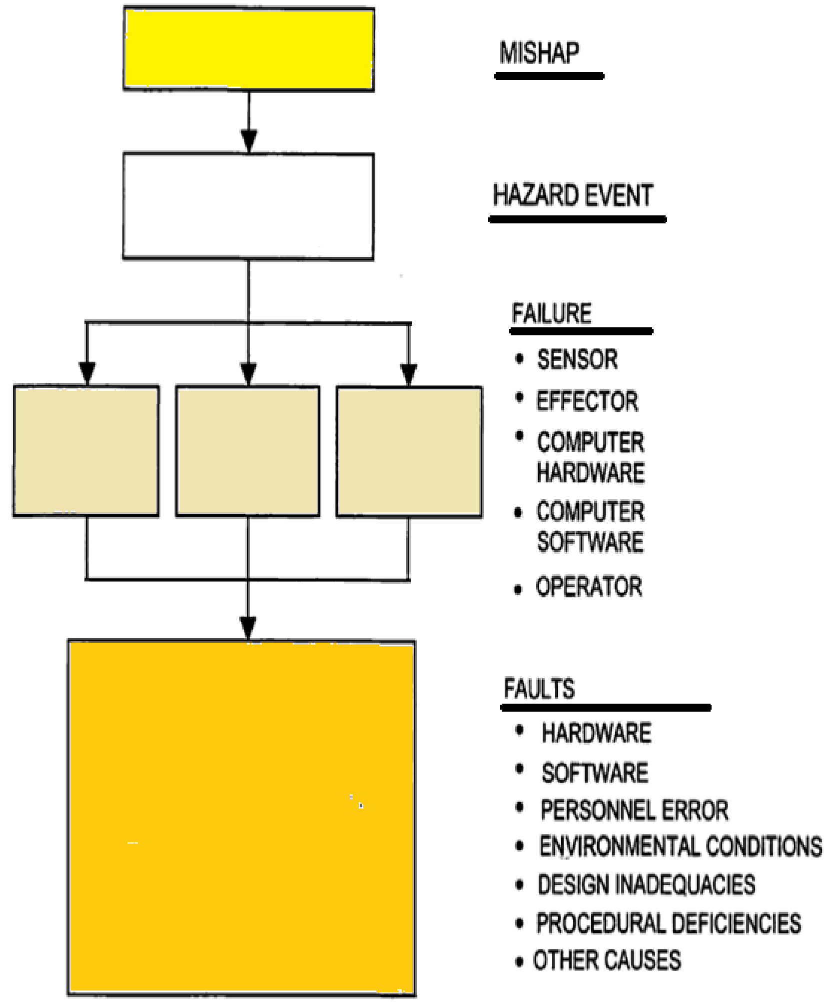
- "Failure"
  - A failing to perform a duty or expected action → Mission related
  - The result of an activated fault or other cause
- "Fault"
  - A defect
- Example: Failure vs Fault
  - A system employs computer-actuated safety valve that closes if computer senses a hazardous event
  - Event occurs, computer senses and signals valve to close
  - Valve may experience *failure* (may not close) due to *fault* of worn bearing (hardware fault), missing spring (maintenance deficiency), or excessive ambient temperature (environmental condition)
- Severity of Component Fault and Failure
  - NOT Severity of the component fault or failure BUT severity of a mishap a fault may cause
- In safety-critical systems, mishap risks are unacceptable → need mitigation step

Hazard Identification – Class Activity

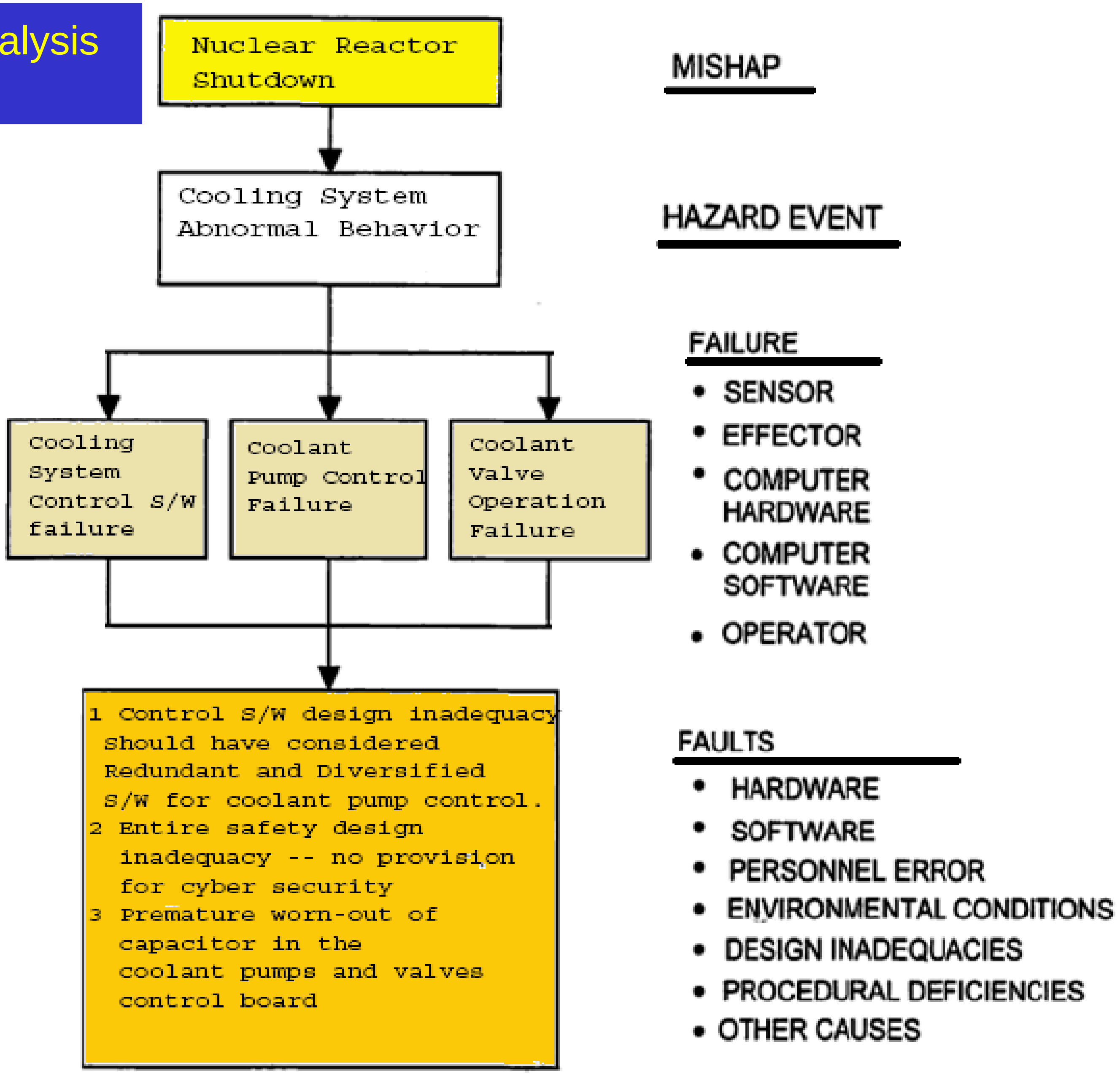
- Work on the subject we did for "system definition" of an automobile electronic control system
  - 1. Choose 1 mishap ("Accident")
  - 2. Identify at least 2 hazards (potential problems that may lead to, or) associated with the mishap
  - 3. Determine the causes of the hazards
  - 4. List failures
  - 5. Narrow down to component faults

Hazard Identification/Analysis Example

- We do not use FTA or FEMA yet
- System (application): Nuclear Power Plant Safety
  - Mishap: Reactor Shut Down
  - List of Hazards
    - (1) Cooling system abnormal behavior
    - (2) On-site Electricity Outage
  - Fill out the mishap-cause tracking chart for EACH of the mishaps

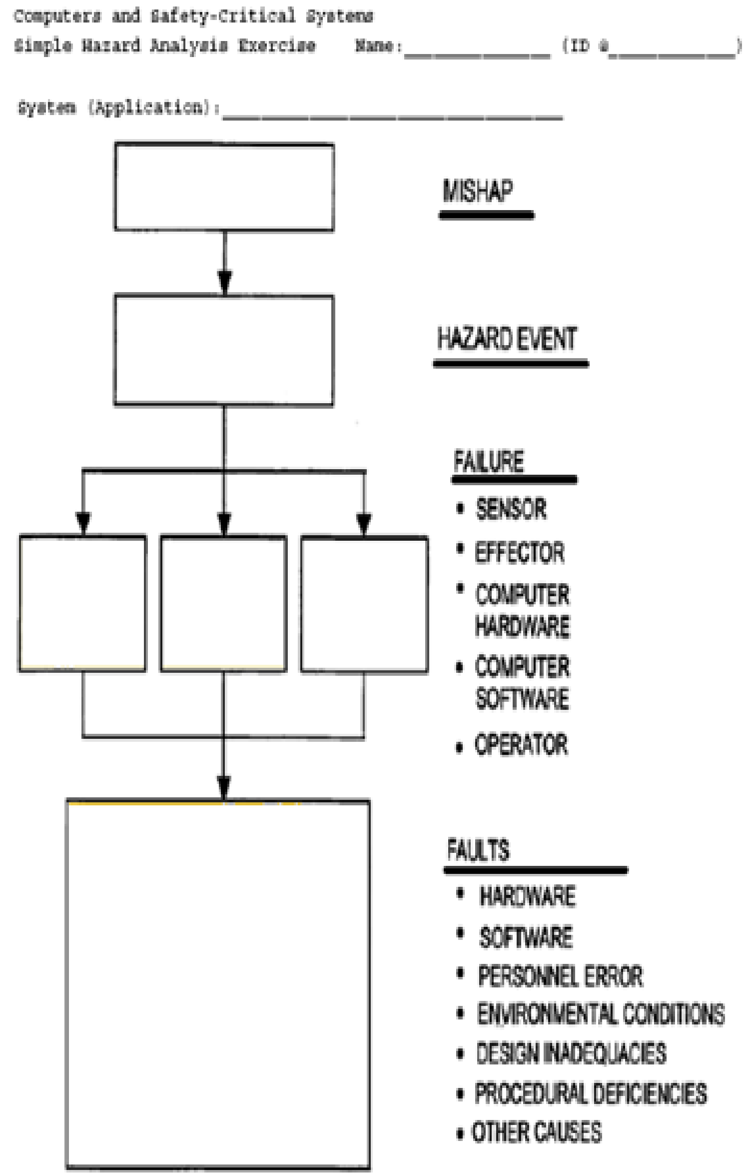


Simple Mishap Analysis - Example



Hazard Identification – Class Activity

- From the "system definition" of an automobile electronic control system
  - 1. Choose 1 mishap ("Accident")
  - 2. Identify at least 2 hazards (potential problems that may lead to, or) associated with the mishap
  - 3. Determine the causes of the hazards
  - 4. List failures
  - 5. Narrow down to component faults
- Fill the chart for Each of the Hazards (with the same Mishap)
- Submission of 2 charts

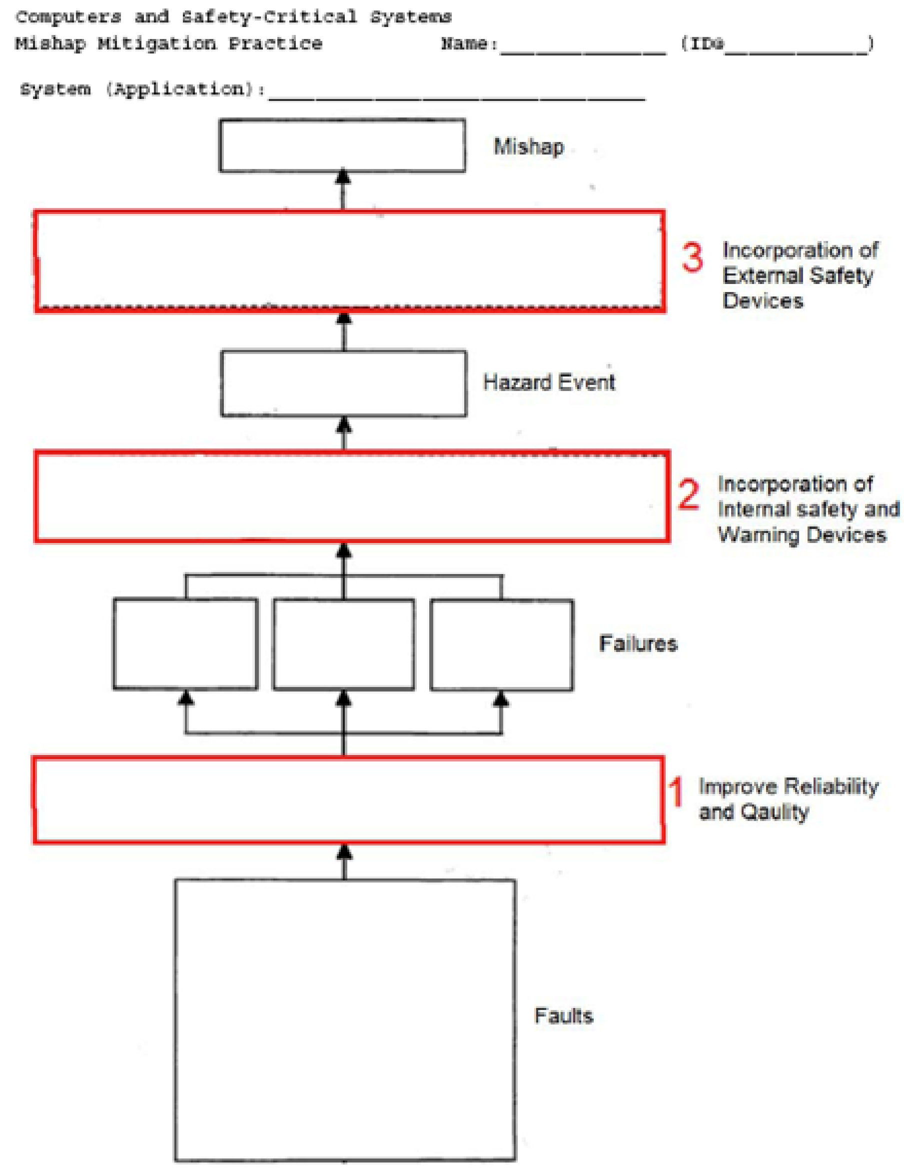


Step 3. Mishap Risk Mitigation

- General Systems
  - MIL-STD-882D requirements specify the approach to be followed for reducing the risk of a given system to an acceptable level.
  - The basic approach is Mishap Risk Mitigation
    - Identify potential mishap risk mitigation alternatives and expected effectiveness of each alternative and method
  - System design order of precedence for mitigating identified hazards
    - Eliminate hazards
    - Incorporate safety devices
    - Provide warning devices
    - Develop procedures and training

Step 3. Mishap Risk Mitigation

- Computer Systems
  - 3 mishap risk mitigation measures that together can reduce mishap risk to an acceptable level
    - Improve component reliability and quality (1)
    - Incorporate internal safety and warning devices (2)
    - Incorporate external safety devices (3)

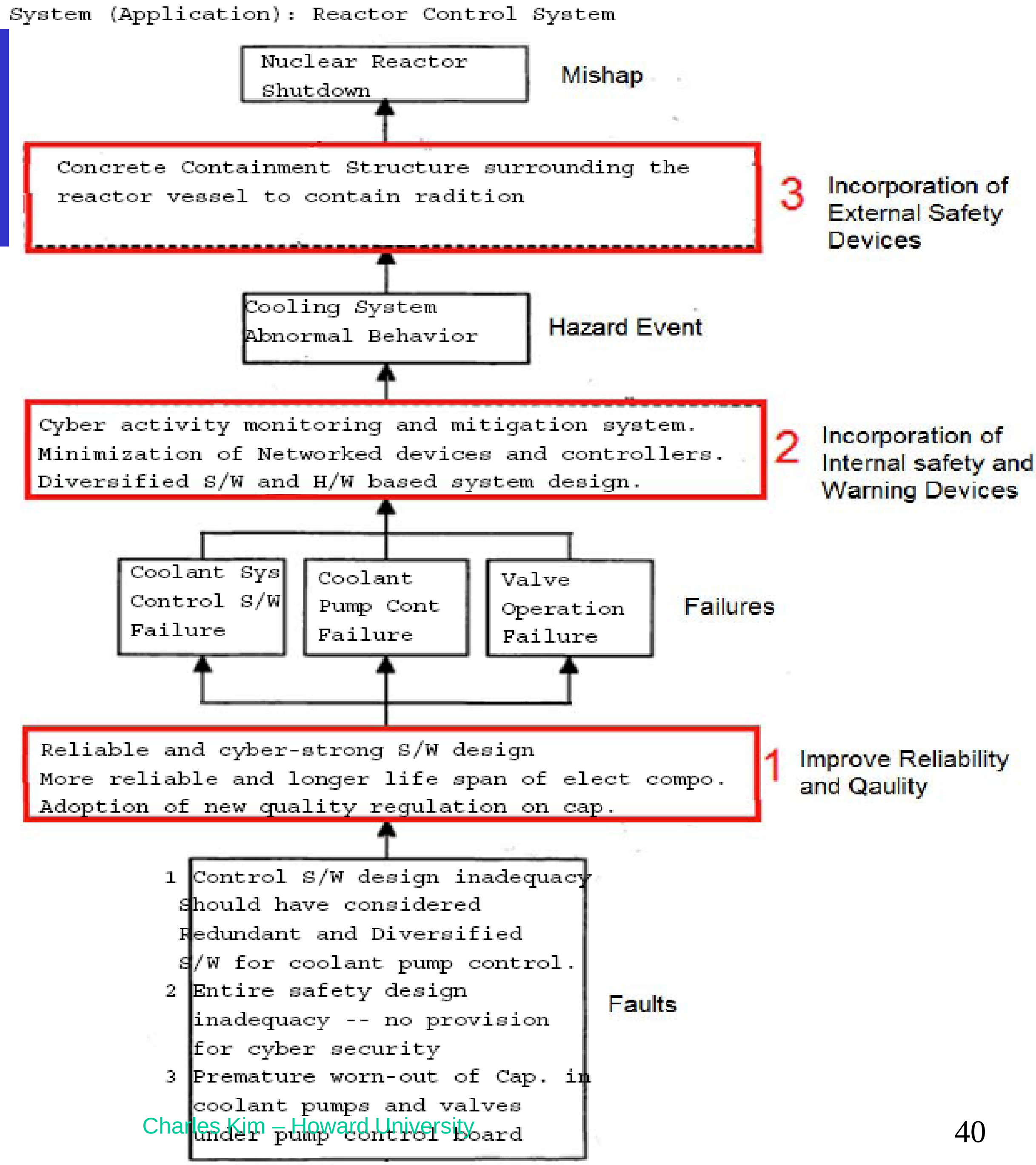


Mishap Risk Mitigation Measures

- Improve Reliability and Quality
  - Improve component reliability: reduce the probability of component failure → reduce the probability of mishap → redundant hardware and software components
  - Exercise quality measures that will avoid or eliminate faults and other sources of component failure
- Incorporate Internal Safety Devices
  - The next line of defense
  - Devices placed inside the computer system
  - Hardware and software
- Incorporate External Safety devices
  - Physical containment
  - Last line of defense
  - Placed outside the computer system
- Applying Mishap Mitigation Measures
  - Apply all the mitigation measures
  - Distribute effort across all three risk mitigation measures in balanced manner

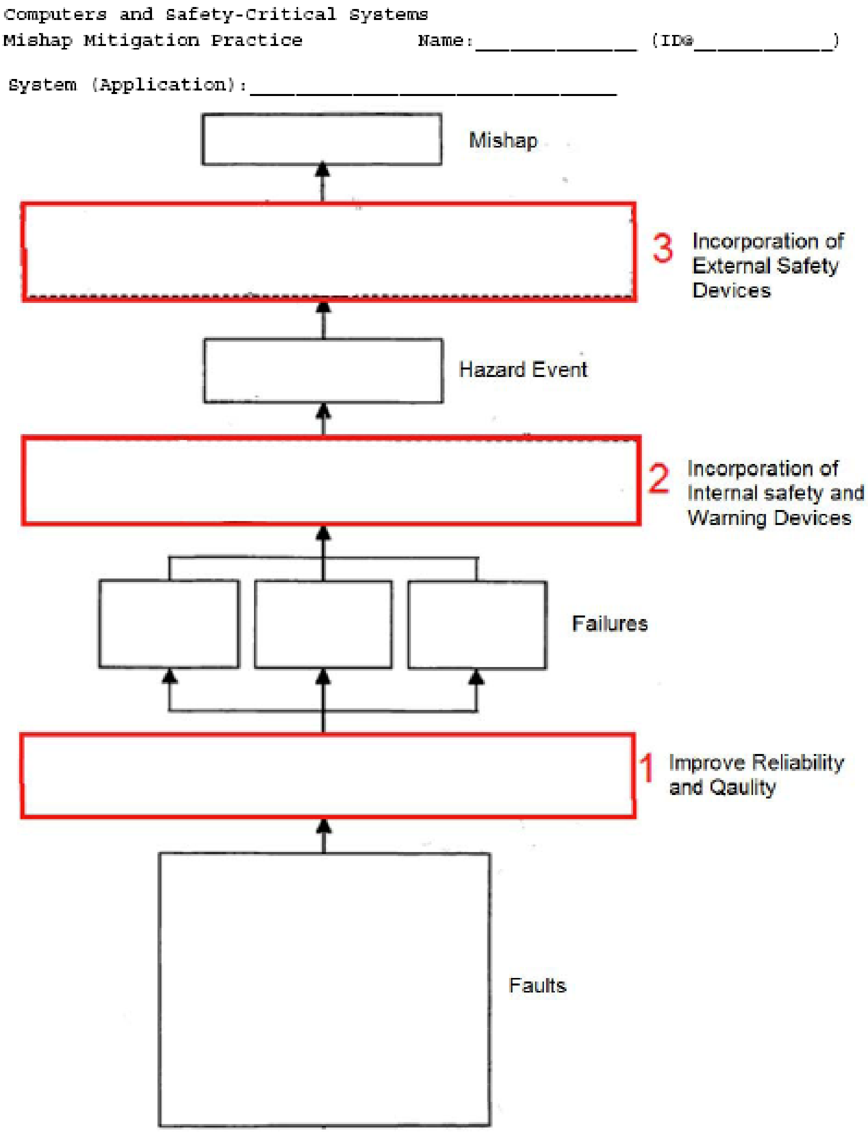
Mishap Mitigation - Example

- Fill out the **red boxes** from the Hazard Identification and Analysis chart



Mishap Mitigation – Class Activity

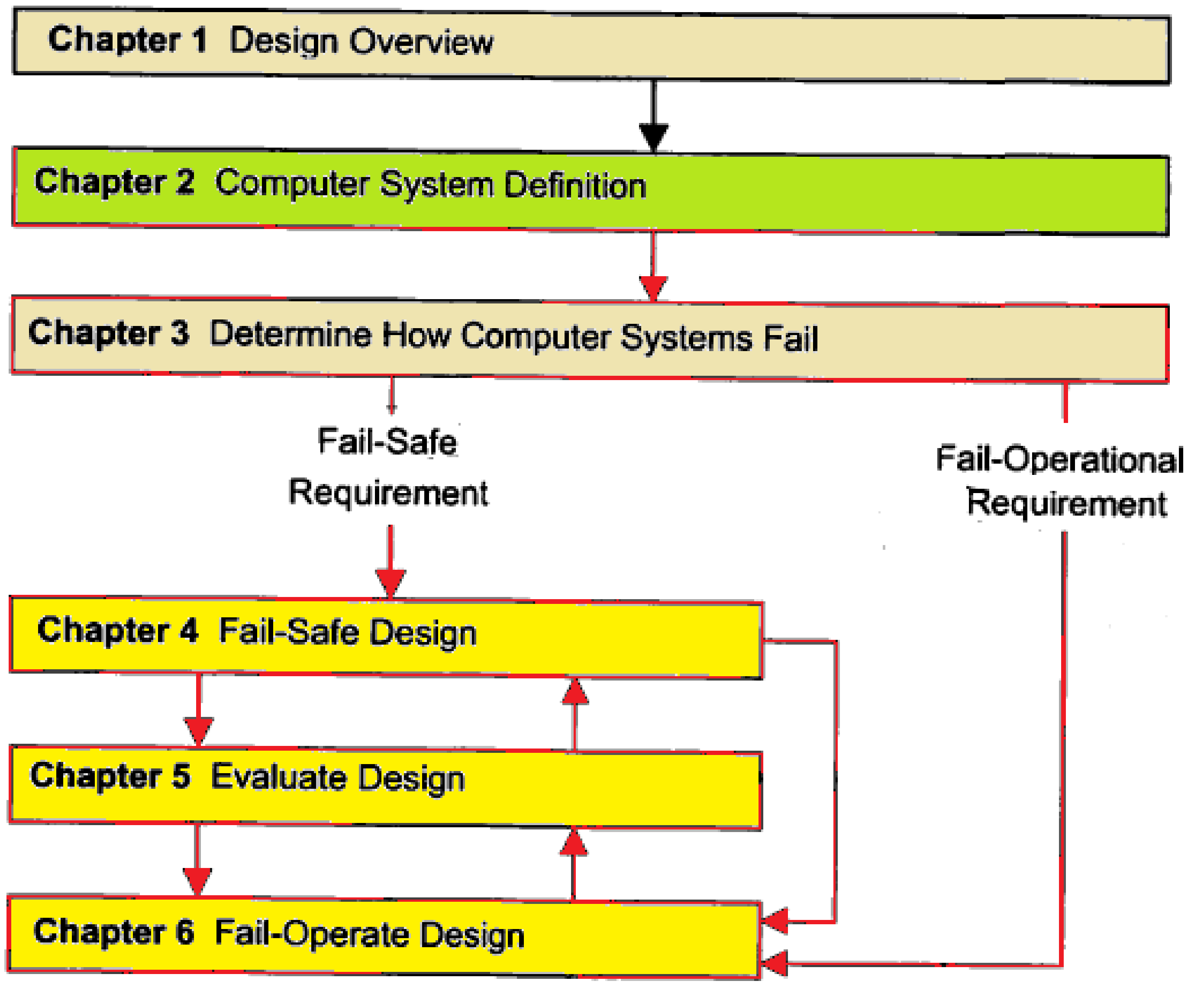
- Start from the Hazard Analysis Charts
- Find ways to
  - Improve component reliability and quality
  - Incorporate internal safety and warning devices
  - Incorporate external safety devices
- Fill out the chart for <u>each of the Hazards</u>
- Take 20 minutes
- Submission of <u>2 charts</u>



Step 4. Mishap Risk Estimation and Acceptance

- Mitigation is an iterative process – with additional design modification until the desired level of acceptable is achieved
- At each iteration, one needs to know (1) how to estimate mishap risks and (2) what constitutes acceptable level of risk
- Mishap Risk Estimation (chapter 5):
  - for a given basic system,
  - estimate individual failure probabilities for the systems' hardware faults, software faults, and systematic failures (e.g., personnel error, design inadequacies, procedural deficiencies, etc.) and
  - then combine these probabilities to arrive at an overall estimate of potential mishap risk.
- Mishap Risk Acceptance
  - Is the mishap risk probability acceptable?
  - Note: Achieving a calculated risk probability less than that required does not guarantee safety: it only indicates that the design (not the final system itself) is safe → validation and verification, testing, simulation, inspections, tests, field trials should be include for assurance.

Subject Organization



Assignment #2

- Search and find one (1) computer-system (hardware, software, or both) caused accident which occurred after January 2011, and describe:
  - (1) the computer system (in terms of application, inputs and outputs, and operator),
  - (2) normal (expected) functions and operations of the computer system,
  - (3) guess and list the hazards (which possibly led to) the mishap (accident), and
  - (4) what failures and/or fault in the component of the computer system might cause the hazards.

Assignment #2 – Submission Requirement

- **Submit by September 25 (Thursday) – Typed Report**
  - A descriptive typed-report of 2 - 3 pages
- **Submit by September 29 (Monday) 9:00pm – Slide File (ppt or pptx)**
  - 6 slides:
    - p1 - Brief on the accident (with Title, Name, and ID);
    - p2 - Computer System;
    - p3 - Normal functions and operations of the computer system;
    - p4- List of hazards and description;
    - p5- Failures and faults that might lead to the hazards; and
    - p6- Conclusions
- **September 30 (Tuesday)**
  - Invited Presentation of selected works

Grading Points

- Grading/Score points (100%)
  - Is this truly computer-caused mishap? (100 or 0)
    - Does the first paragraph of the report satisfactorily summarize the entire report? (20%)
    - Is the computer system well researched and satisfactorily described? (20%)
    - Are functional and operational behaviors of the computer system under normal condition well described? (20%)
    - Are the hazards adequately listed and described? (20%)
    - Are the failures/faults adequately described which might lead to the hazards? (20%)
  - Presentation points (extra 25%)