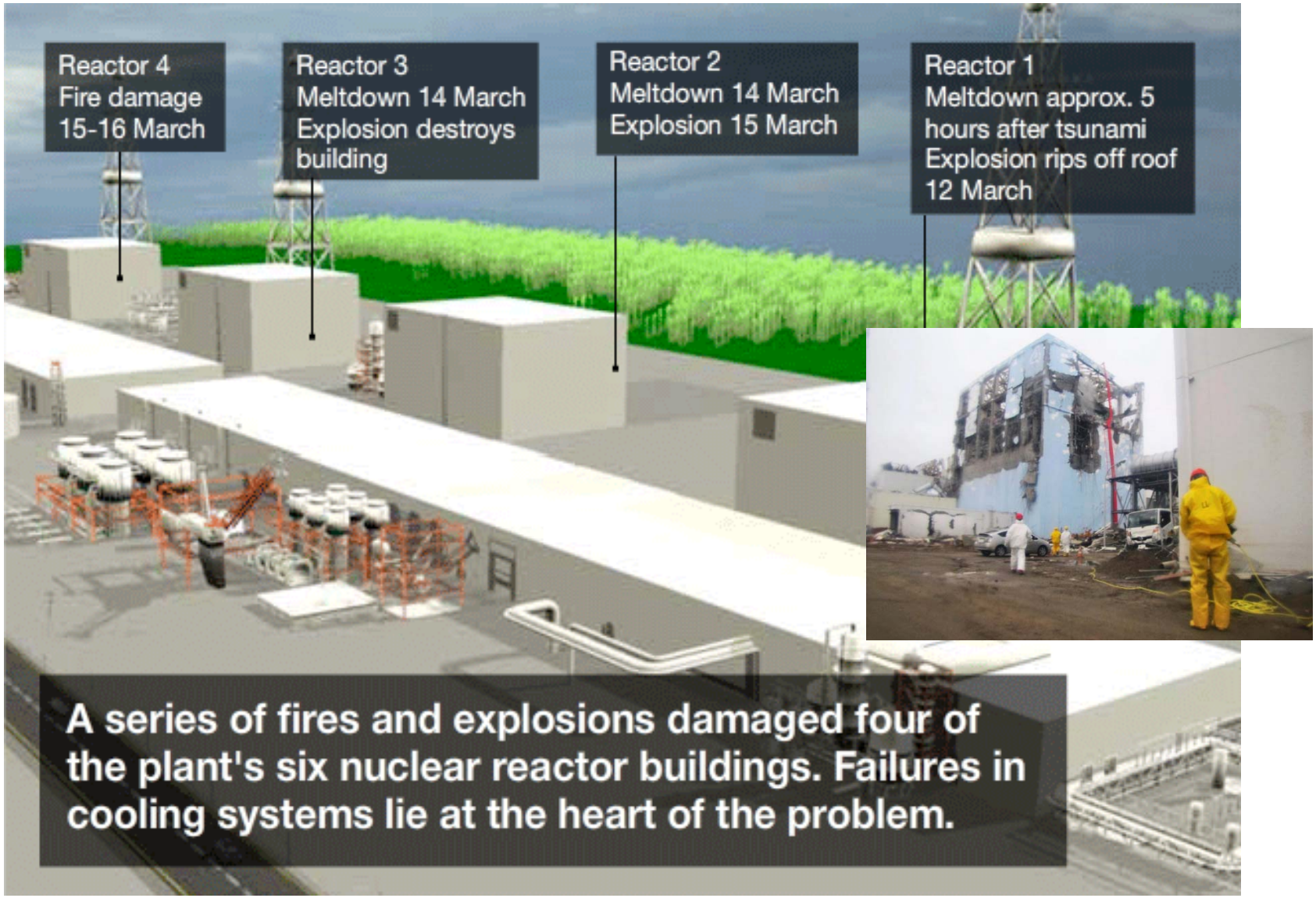
EECE 692: System Safety Spring 2012

- Coincidence that we start the new course with the Costa Concordia?

What went wrong?



So many software bugs. No Wonder…

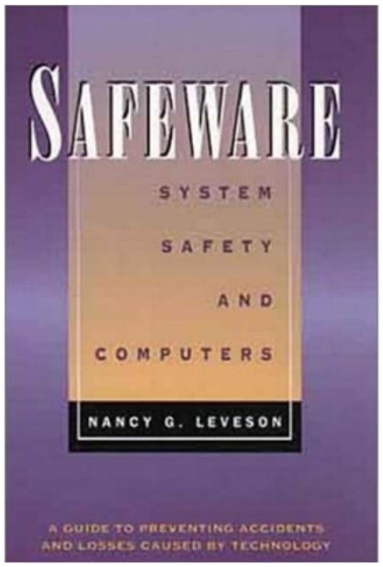
Goals

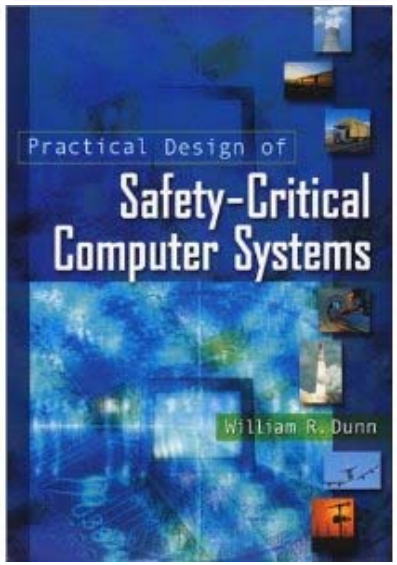
- Objectives
  - Basic Understanding and Practical (indirect, though) Experience of System Safety Activities for Safety-Critical Systems, Cyber Physical Systems, and Complex Systems
- Focuses
  - Safety-Critical Computer Systems
  - Software Safety
  - System Safety Interface
    - Reliability
    - Risk Analysis
    - Human Factor
    - Safety Management and Control
    - Quantification of Safety

System Safety Spring 2012

- **EECE 692**
  - CRN 16105
  - 3 credit hours
  - R 3:30 – 6:20 pm
  - LKD 3105
- **Instructor**
  - Dr. Charles Kim
  - (202)806-4821
  - ckim@howard.edu
  - Office Hours (LKD3014)
    - M & T 3:00 – 5:00 pm
    - R 2:00 – 3:00 pm
    - Scheduled appointment

Required Textbooks





- **Textbook 1**
  - "Safeware – System Safety and Computers" by Nancy Leveson
  - Addison-Wesley
  - ISBN: 0-201-11972-2
  - *NOTE: Used book is cheap
- **Textbook 2**
  - "Practical Design of Safety-Critical Computer Systems" by William R. Dunn
  - Reliability Press.
  - ISBN 0-9717527-0-2
- **Other Resources**
  - Handouts on Reliability Calculation
  - Book excepts
  - Articles
  - Reports

Language of System Safety

- Latin " Salvus"
  - Safe, whole, healthy
  - Try Google Translate: "Salvus Sis"
- Webster Dictionary:
  - SAFE: "**freed from harm, injury, or risk; no longer threatened by danger or injury; secure from threat of danger, harm or loss**"
  - SAFETY: "**the condition of being safe; freedom from exposure to danger; exemption from hurt, injury or loss**"
- DOD Mil Std. 882
  - "System Safety Program for Systems and Associated Subsystems and Equipment"
  - SAFETY: "**Freedom from those conditions that can cause injury or death to personnel, or damage to or loss of equipment of property**"
- Discussion on the definition of "Safety"
  - Definition is very general: people and things
  - Definition is qualitative rather than quantitative in nature:
  - Definition permits a natural interface between safety and those other disciplines closely aligned with safety: System effectiveness, reliability, maintainability, quality assurance, human factor

Quantification of Safety

- Quantification is necessary for a consistent and reliable estimate about the safeness of undertaking a given task
- Example
  - Changing Lane
  - Assessment of circumstances
  - Decisions
    - Do not change the lanes at this time
    - It is safe to change lanes
  - Accident caused by errors in assessment
  - Addition of sensing devices after study by NTSB, etc, with quantitative assessment
- Quantification in Safety Domain (2 ways)
  - **Probability** assignment to each of a set of events and then combined into an overall probability --- Good when effects of an event are known but its likelihood of occurrence is not
  - Establishment of the effects of an event in terms of **intensity**: As in the danger of electrocution from contact with electricity as low as 10 mA

Hazard Considerations

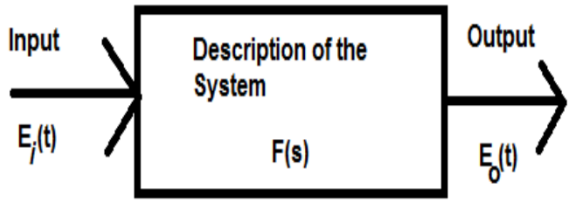
- Hazard
  - Antithesis of “Safety”
  - Villain of “System Safety”
  - Ubiquitous in real life
- Definition
  - “**A potential condition which may result in injury or death to personnel, or damage to or loss of equipment if property**”
  - Qualitative !!! like the definition of Safety
- Quantification
  - Quantification of ***potential***, probabilistic problem.
  - Assessing the seriousness of the injury or damage
    - More complex due to relative judgment involvement in, especially, human survivability
- Classification of Hazards
  - As a function of resulting severity on /**equipment damage/personnel injury**
  - **Causes**: **(1) human error, (2) deficiency of inadequacy of design, (3) equipment malfunction**
  - **Class I. Safe** /No equipment damage/no personnel injury
  - **Class II. Marginal** /Minor equipment damage/No personnel injury
  - **Class III. Critical** /Substantial equipment damage/transient (recoverable) injury
  - **Class IV. Catastrophic** /Systems loss/irreversible injury or death

Hazard Vector

- Hazard level associated with undertaking a given task is
  - A function of
    - The **severity** of the hazard's effects (or class), C
    - The **probability** that the hazard will occur, P
  - Hazard Level (HL)
    - HL=f (C_i, P_i)
    - C_i: weighting factor associated with i^{th} hazard
    - P_i: Probability that the i^{th} hazard will occur
  - Appropriate Strategy?
    - Minimization of HL

System

- Definition of System:
  - "**a device, scheme, or procedure which behaves in accordance with sine description, its function being to operate on information and/or energy and/or matter in some time reference in order to yield information and/or energy and/or matter**"
  - No restriction on the size or complexity
  - "Mission" – operational role of a system
- Description of System (or "Specification")
  - Inputs, $E_i(t)$
  - Outputs, $E_o(t)$
  - States of the system (system phase space)
  - A description model F(s)
    - Steady and Transient States of the System



System Safety

- "System safety is concerned with providing procedures and equipment for preserving the integrity of a system over the range of environmental and operational conditions that can reasonably be expected to occur during the mission"
- 2 fundamental aspects to a formal definition:
  - identification and control of hazards ("safety" part of system safety)
  - Expectation (anticipation, "reasonably expected") or reasonableness ---- determination of what is reasonable or acceptable for a given set of circumstances, because absolute safety can never be achieved. ("system" part of system safety)

Definition of System Safety

- Definition with aspects of Control+Reasonableness
  - "An optimum degree of safety, established within the constraints of operational effectiveness, time, and other applicable interfaces to safety, that is achievable throughout the life cycle of a system"
  - Reasonableness (qualitative) → optimization (quantitative)
  - Optimization: "the application of mathematics and simulation techniques for identification, examination, and calibration of the interactions between and among the elements of a system"

Optimizing System Safety

- Optimum degree of safety requires
  - Scientific knowledge and method in assisting decision-making among alternatives and configurations
  - Example configurations
    - Minimum complexity and minimum demands on human skills for operation and maintenance
    - Redundancy such that the failure of any one component cannot lead to incapacitation of the system of to personnel fatality
    - Provision of indicators for those components that have become degraded and, consequently, are likely to fail
- Optimization means that safety may have a **value** which varies from person to person and that it may be variable for the same individual under different circumstances → **subjective** optimization !!!

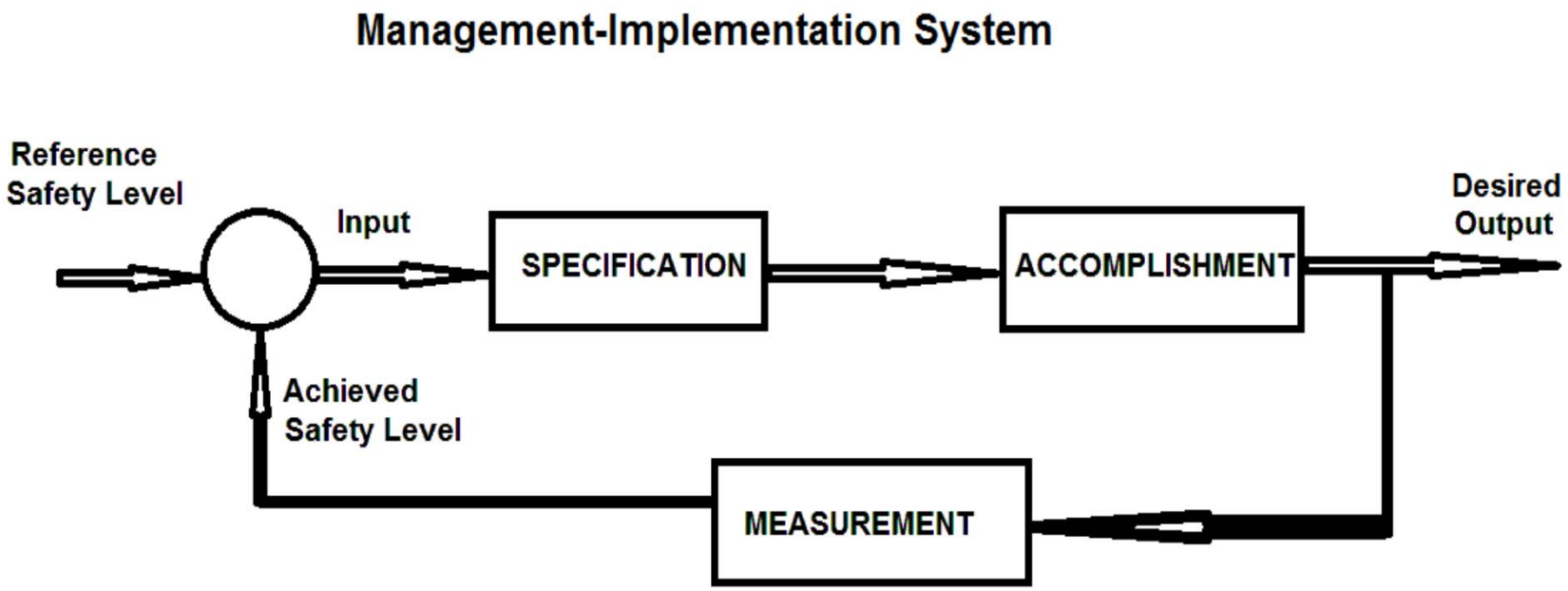
Value of System Safety

- Absolute Value: "Cost(price) value is equal to the amount of money needed for purchasing labor, material, and overhead that are required to produce a given item or establish and explicit system output"
- Relative Value: subjective (use value or esteem value)
  - "Use value relates to the properties and qualities of an item or system output that permit a task, work, or a service to be performed."
  - "Esteem value relates to the characteristics of an item or a system output that make the system desirable or attractive and, consequently, valuable."
- Combined meaning with absolute and relative values
  - "Exchange value is determined by the intrinsic properties of an item or system output which enables it to be exchanged or traded for some other item or output"
- Transformation of relative value into absolute value?
  - Via game theory → fault tree analysis
  - In all, some quantitative assessment of the risks must be preceded before taking any action → need some transformation of relative safety values into absolute ones.

Managing for System Safety

- Achieving an optimum or acceptable level of safety depends to a large degree on system safety management and system safety implementation
- System Safety Management: "System safety management is that element of program management which assures the accomplishment of the system safety tasks including identification of the system safety requirements; planning, organizing and controlling those efforts which are directed toward achieving the safety goals; coordinating with other (system) program elements; and analyzing, reviewing, and evaluating the program to assure effective and timely realization of the system safety objectives."
- System Safety Implementation: "System safety implementation consists of those activities carried out for the application of scientific principles needed for the timely identification of hazards and for the initiation of those actions necessary to prevent or control the hazards that are determined to be inherent in the system"
- The two are engaged with a feedback loop of **Specification, Accomplishment, and Measurement.**

Management-Implementation System



- If "Achieved Safety Level" > "Desired Output", what do we do?
  - Is resource misallocated?
  - Is the aim too low?

Nature of Safety Domain

- System Safety is concerned with:
  - Identification of hazards
  - Determination of optimum or acceptable safety-levels
  - Elimination or minimization of known hazards
- Ideal situation
  - All possible hazards concerning a given system along with their likelihood are known on an a priori basis → Safety level is known with certainty → Determine if the risk is acceptable →Increased allocation of system safety management and implementation resources
- Real situation
  - All hazards are not known
  - The likelihood of the know hazards are not certain
  - System management and implementation are not independent from other system activities → System Safety interfaces

System Safety Interfaces

- Interfaces with all disciplines that are involved in the **Design, Development, and Operation** of the system under consideration
- System point of view in the relationship between a system and the system safety:
  - **System objectives**
  - **Effectiveness**
  - **Mission effectiveness**
  - **System effectiveness**

- System Effectiveness: "**The measure of the extent to which a system may be expected to achieve a set of stated system objectives"**

System Effectiveness

- **Disciplines** considered in the (sub-) optimization of system effectiveness:
  - Safety S
  - Reliability R
  - Maintainability M
  - Human Factors H
  - Value Engineering V
- Functional Relationship, E(t)
  - E(t)=f{(Sa/Ss), (Ra/Rs), Ma/Ms), (Ha/Hs), (Va/Vs)}

    a: the **achieved level** of each parameter at some specified time in the system's life.

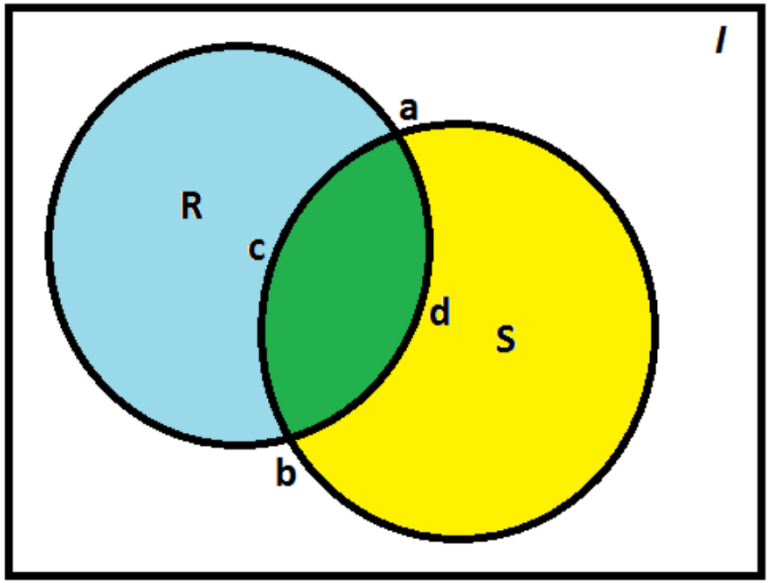
    s: the **specified level** established for the parameter.
- Fundamental Problems of E(t)
  - The components of E are never completely independent of each other
  - Availability? ← maintainability; survivability? ← reliability (and/or safety)
  - The component have different utility values

Interface with Reliability

- System safety is most closely related with Reliability than other components
- Reliability: "Probability that the system will perform its intended function for a specified period of time under a set of specified environmental conditions"
- Safety: "Freedom from those conditions that can cause injury or death to personnel and damage to, or loss of, equipment or property."
- **"Hazards which occur without causing injury or death to personnel" → domain of safety or reliability?**
- **"A hazard which affects only personnel" → domain of safety or reliability?**
- Fusion of safety and reliability:
  - Quantification of safety: **Safety expressed in probability that injury or damage does not occur.**

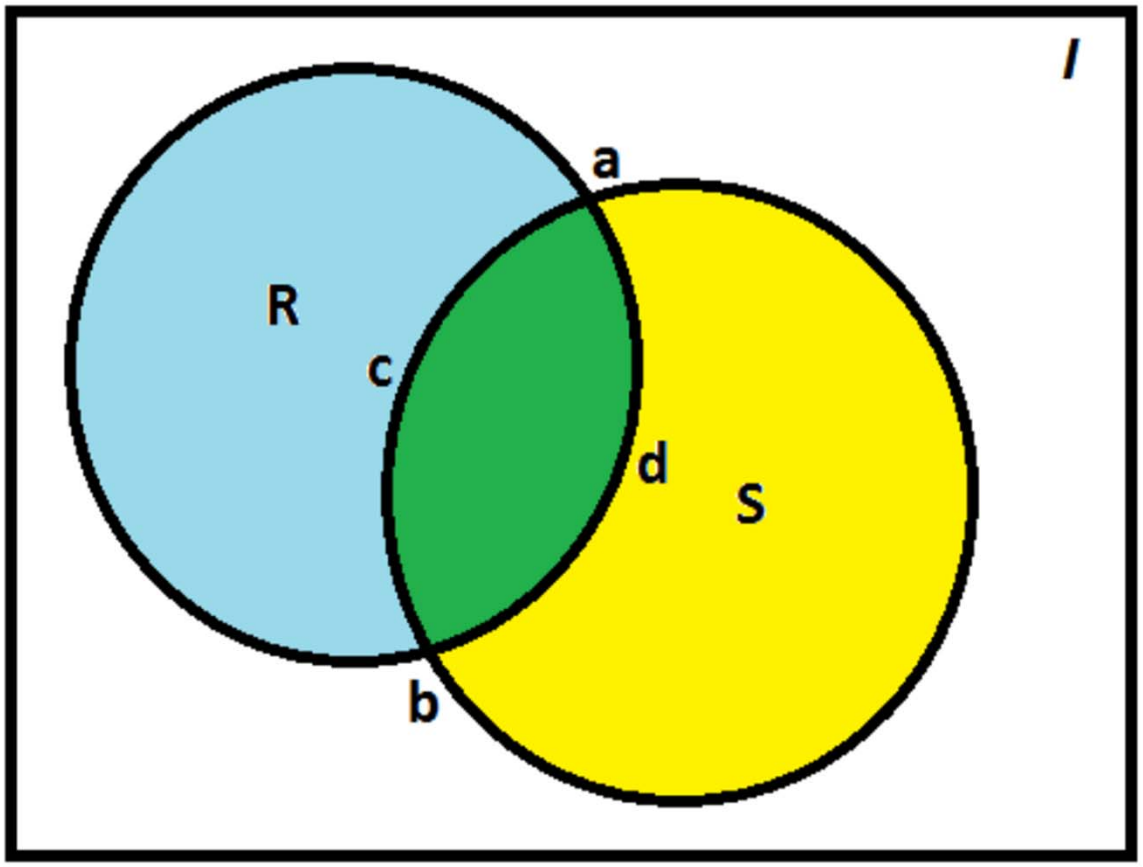
Safety-Reliability Interface

- S: Safe event
- R: Reliable event
- Example (sample point marking??)
  - Safe arrival
  - Damage to car but no injury
  - Injury but no damage to car
  - Injury plus damage to car
- How about this?
  - An engine does not start →no driving & no accident
  - A collision caused by careless driving



Safety-Reliability Interface

- Usually, improvement in reliability improves in safety → reliability aspects must be included in safety improvement
- Common goal:
  - expansion the area of {S^R}



Reliability vs. Survivability

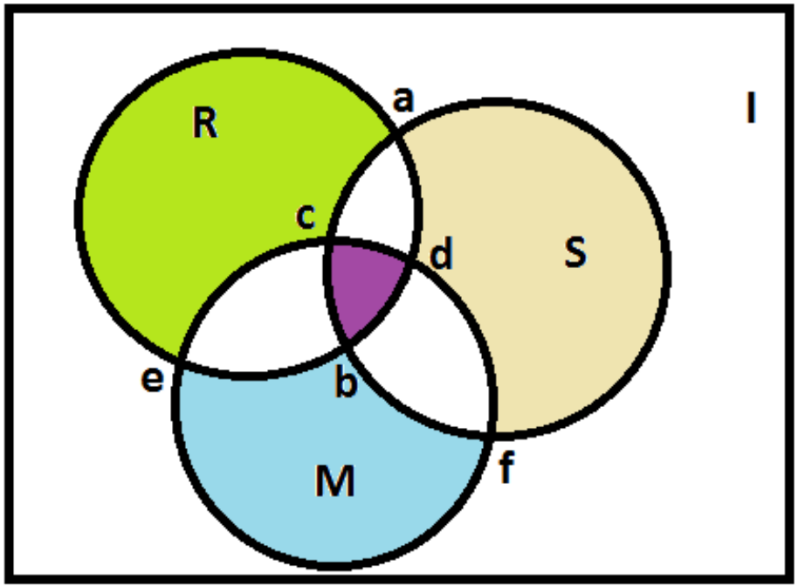
- Survivability
  - A variant of reliability
  - Definition: "The measure of the degree to which a system will withstand the environment in which it is placed and not suffer abortive impairment of its ability to accomplish the designated mission."
- Reliability vs. Survivability
  - Reliability: relates to activity carried out prior to the appearance of failures or degradation in accordance with a priori standards
  - Survivability: relates to activities conducted subsequent to the occurrence of failure or degradation
  - What can be unreliable and still survive?
- Situation Dependency (example. Multi-engine commercial aircraft): Conflict and Compromise
  - Reliability requirement: each engine must assure the safety of the aircraft → affects design and maintenance policies for the engines
  - Survivability criteria: the aircraft must survive in the event of a failure of an engine → design and maintenance policies of engines

Interface with Maintainability

- A characteristic of system design, installation, and operations
- Definition: "The probability that the system will be retained in, or restored to, a specified condition within a given period of time, presuming that the maintenance is performed in accordance with a set of prescribed procedures and allocated resources."
- Maintenance: "all actions necessary for retaining the system in, or restoring it to, a specified condition"
- Maintenance for retaining a system in sound condition → preventive in nature
- Maintenance carried out for restoring a system from difficulty → corrective in nature
- Fundamental role of maintainability is to increase system life without necessarily enhancing safety

Safety-Maintainability-Reliability Interface

- Mark the following guidelines:
  - Direct removal and replacement of faulty components, or their repair by personnel in situ → S^M
  - Switching to redundant equipment through remote means such as telemetry, or in situ by attending personnel → S^M
  - Switching to redundant equipment through the use of built-in, self-checking circuits: S^M^R
  - Redundancy used in majority voting, or in a fail-safe configuration, for replicated elements → S^R



Availability

- Relates both reliability and maintainability
- Definition: "The probability that a given system is in an operable state and can be committed at a given instant of time"
- The state of being operable generally implies that an inoperable item can be restored to an operable condition by means of maintenance activities
- A (availability) = MTBF / [MTBF + MTTR]
  - MTBF: mean time between failure
    - (total functioning life (time)) / (total number of failure)
  - MTTR: mean time to repair
    - (total time required for corrective maintenance) / (total number of corrective maintenance actions)

Interface with Human Factors

- Personnel activities and incidences of human error
- Human factor: "A body of scientific facts about human characteristics. The term covers all biomedical and psychological considerations. It includes, but is not limited to, principles and applications in the areas of human engineering, personnel selection, training, life support, job performance aids, and human performance evaluation"
- Human Engineering: "The area of human factors which applies scientific knowledge to the design of items in order to achieve effective man-machine integration and utilization"
- Human Performance: "A measure of human functions and actions is a specified environment"

Safety and Human Factor

- Problems (in safety enhancement)
  - Much of the biological and psychological information needed for the purpose is not yet available
  - The mathematical tools for quantifying and optimizing in a formal fashion are just now being developed
- Fundamental areas in which human factors and system safety interface
  - The mechanisms by which the body regulates and maintains an optimal internal environment
  - Person's ability to adapt to specific work-sleep schedules while maintaining effectiveness.
  - Human tolerance to physical forces such as shock, vibration, and noise
  - Human tolerance to long-term effects of irreversible, or slowly reversible, pollutants expended into the environment.

Interface with Value Engineering (or value Analysis)

- Value Engineering: "an organized effort to analyze the functions of systems, equipment, facilities, services, and supplies for the purpose of achieving essential functions at the lowest life-cycle cost consistent with required performance, quality and safety."
- Safety has a value
- Problem of a relative value as a factor to be quantified
- Transformation of relative safety values to absolute values – complete safety analysis
- Value transformation in economics: relation between relative and absolute values in mathematics based on supply and demand laws – Augustin Cournot

Value Engineering and Safety

- Some explicit dollar value is assigned to a system for each significant inherent hazard known to exist → All relative values which affect the inputs or outputs of the system have been transformed into absolute values.
- The cost of eliminating a single hazard is relatively small when there are a large number of hazards inherent in a system
- The cost becomes relatively large as the number of inherent hazards remaining in the system approaches zero.
- It would need an infinite amount of money to eliminate all hazards
- Assessment of the value of safety in absolute terms – cost

Car, Value Engineering, Software

- Value Engineering in auto industry

Game Theory and Value of Safety

- One method of transforming relative values into absolute terms
- “utility” = payoff (game)=value (economics) = “output” in system safety
- Game: players, strategies, and payoffs
- The value of the payoffs in a game depends on both absolute and subjective considerations of its value.
- Example: 3 players with 3 payoffs 0.9, 0.7, 0.2
  - Cf. Safety terms: likelihoods of a given hazardous event occurring in accordance with a strategy selected.
  - Intervals of the payoffs are: 0.2 and 0.5
  - Invariant of payoff in transformation
  - Adding 0.05 to each of the payoffs does not change the interval of the payoffs: payoff=“utility of the interval scale”
  - No change in the utility of the payoffs
  - But the likelihood of hazard increases regardless of the strategy selected.