Raytheon

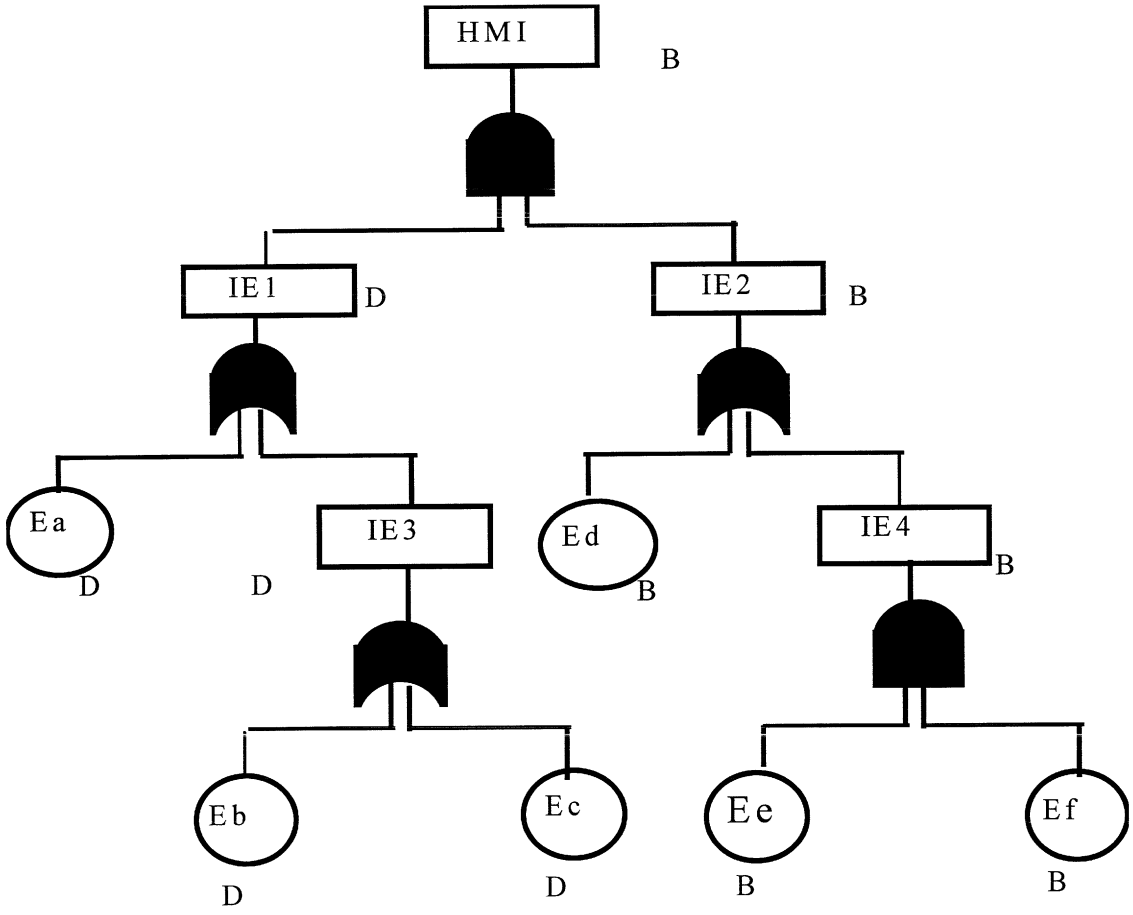
DETERMINING SOFTWARE (SAFETY) LEVELS FOR SAFETY-CRITICAL SYSTEMS

Doris Tamanaha
714-446-3050

Meng-Lai Yin (Presenter)
714-446-4269

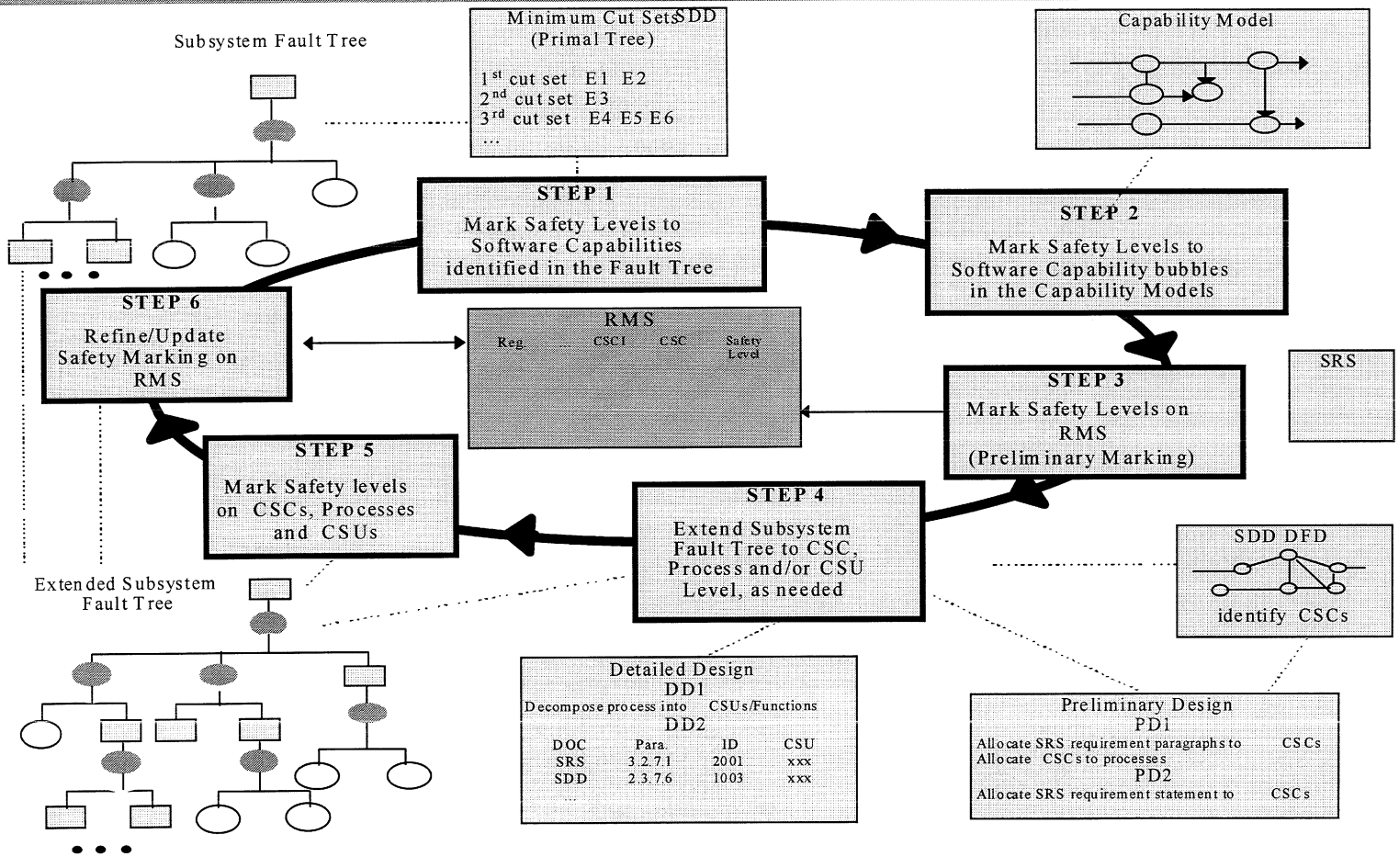
Raytheon

Example Fault Tree



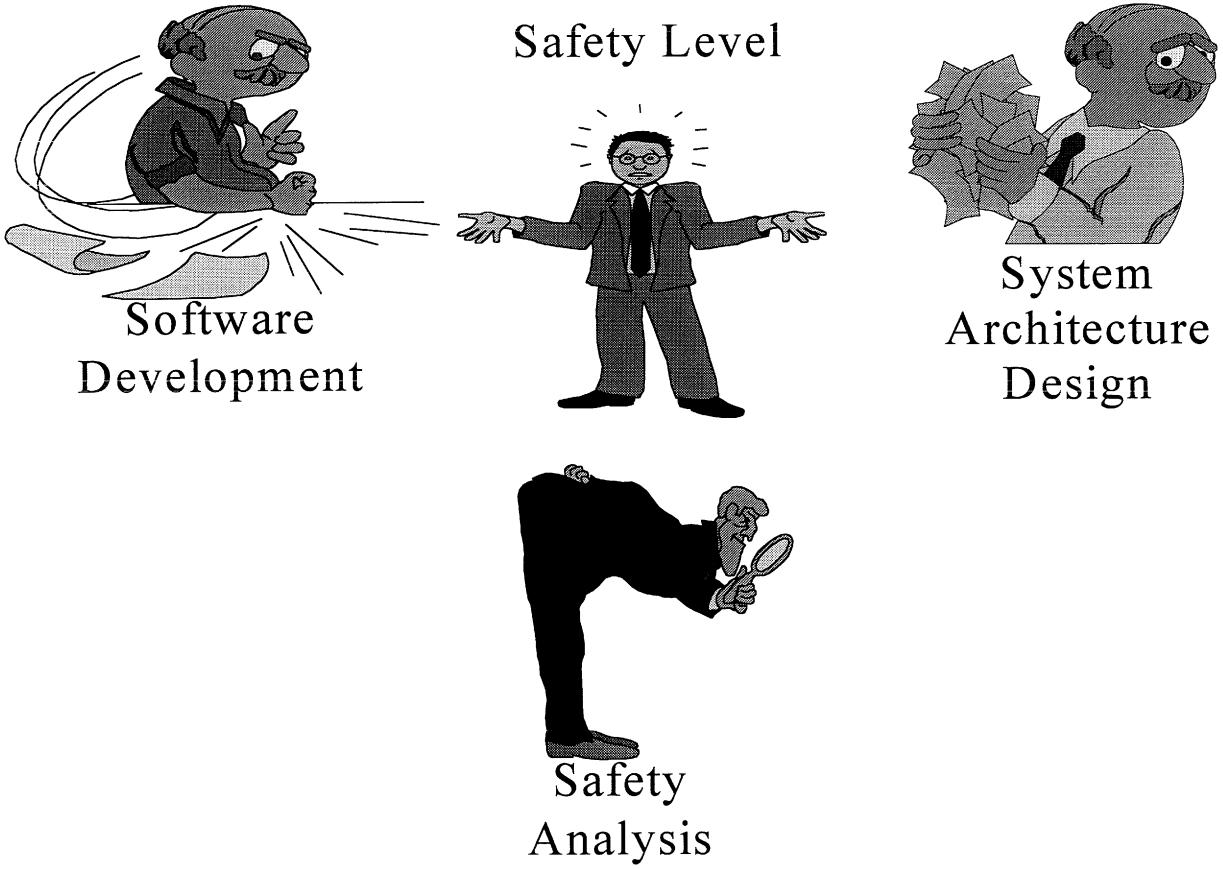
Software (Safety) Level Determination Marking Process

Raytheon



Different Views of Software (Safety) Levels

Raytheon



Managing Inconsistency (1)

- Basic philosophy: <u>inconsistency is expected</u>

Thus,

- record all existing software levels
- from this, the inconsistency can be identified
- only if we can recognize the inconsistency can the inconsistency problem be addressed and resolved

Managing Inconsistency (2)

STEP 1.

- maintain different software (safety) levels associated with different organizations (RMS database)
- assure ASL ≤ AAL ≤ DAL

  ASL: Assigned Software Level

  AAL: Assessed Architecture Level

  DAL: Development Assurance Level

Managing Inconsistency (3)

STEP 2.

- Cross-checking the recorded software (safety) levels and identifying the inconsistency areas

STEP 3.

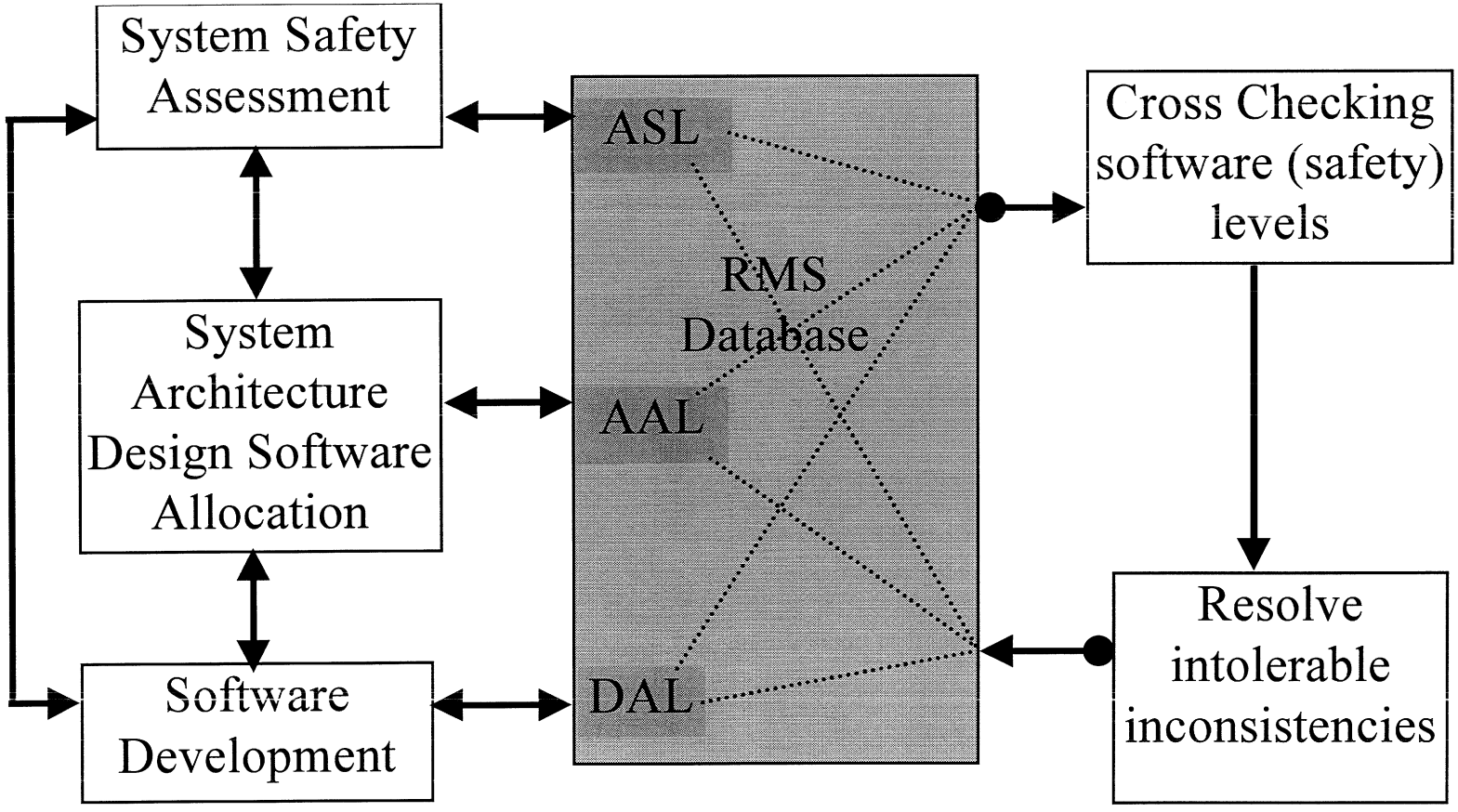
- Resolving the inconsistency by involved organizations and engineers

Types of Inconsistency

- tolerable: software developers follow a process that exceeds the current process requirements
- intolerable: software developers follow a process that does not meet the current process requirements (for safety certification)

Process for Managing Inconsistency

Raytheon



Implementation Results (1)

Raytheon

- 2 types of anomalies: internal and external
- internal (case 1)
  - due to the sharing of the same software by different configuration items
  - different ASLs are assigned for the same software
  - resolved by assigning the highest level

Implementation Results (2)

Raytheon

- internal (case 2):
  - similar design used on different platforms (the platforms have different levels)
  - dual designation (i.e., B/D) are carried for the same software requirements
  - resolved by <u>examining the requirements for two processes</u>

Implementation Results (3)

Raytheon

- External anomalies
  - DAL is N/A, while ASL and/or AAL has a level assigned (example, COTS products)
  - One of the levels has two values assigned, while the others has only one level
  - The DAL is lower than the AAL and ASL
  - * Resolving external anomalies involves corresponding safety engineers, software development team leads, and system engineers (assure ASL ≤ AAL ≤ DAL)

Summary

- The method and the process for Marking Software (safety) Levels
- The Inconsistency Problem
- The philosophy and the method of handling the inconsistency problem
- The implementation results