SAFEWARE ENGINEERING

Engineering For A Safer World®

STPA for a Non-advocate Safety Assessment of the Ballistic Missile Defense System

Grady Lee

Presented to:
The STAMP/STPA Workshop April 18, 2012

SAFEWARE ENGINEERING
Engineering For A Safer World

Today's Goal

- Discuss a safety assessment methodology based on STPA that:
  - Provides an organized, methodical, and effective means to assess safety risk
  - Develops appropriate hazard mitigations regardless of where in the life cycle the assessment is started.

SAFEWARE ENGINEERING
Engineering For A Safer World

Background

- The Missile Defense Agency (MDA) is developing the Ballistic Missile Defense System (BMDS)
  - a layered defense to defeat all ranges of threats in all phases of flight (boost, mid-course, and terminal)
  - Made up of many existing systems (BMDS Element)
    - Early warning Radars
    - Aegis
    - Ground-Based Midcourse Defense (GMD)
    - Command and Control Battle Management and Communications (C2BMC)
    - Others

SAFEWARE ENGINEERING
Engineering For A Safer World

Background (2)

- The first NSA was performed on the Limited Defensive Operations (LDO) BMDS
  - LDO NSA limited to GMD Launch System
- The Block 04 NSA has been completed and had a larger scope than the LDO NSA
- NSA continues for each Block upgrade

SAFEWARE ENGINEERING
Engineering For A Safer World

Background (3)

- The MDA employed the STPA methodology to characterize the residual safety risk of the BMDS
- Many Elements and components are upgrades of fielded systems
  - UEWR
  - CDU

SAFEWARE ENGINEERING
Engineering For A Safer World

Background (4)

- BMDS integrates into a single system a number of programs that had historically been developed as stand alone systems
  - Aegis
  - GMD
  - Others
- The Elements of the BMDS have safety programs, but considerable complexity, coupling, and safety risk is introduced by integrating them into a single system

SAFEWARE ENGINEERING
Engineering For A Safer World

Background (5)

- Successfully conducting a safety assessment required a hazard analysis methodology that:
  - Considers hazards and causes due to complex system interactions (more than just failure events)
  - Provides guidance in conducting the analysis
  - Comprehensively addresses the whole of the system, including hardware, software, operators, procedure, maintenance, and continuing development activities
  - Focuses resources on the areas of the system with the greatest impact on safety risk

SAFEWARE ENGINEERING
Engineering For A Safer World

The Assessment

- A Fictional Missile Intercept System (FMIS) will be used to describe the NSA
  - Similar to programs within the BMDS
  - Suitable for an example of how the safety assessment methodology is conducted and the results achieved at MDA
- FMIS uses a hit-to-kill interceptor that destroys incoming ballistic missiles through force of impact

SAFEWARE ENGINEERING
Engineering For A Safer World

Review System Hazards and System-level Safety Constraints

- The first step of a system-theoretic safety assessment is to:
  - Review the hazards identified for the system
  - Ensure that appropriate system-level safety constraints are in place
- For the FMIS NSA, only inadvertent launch was reviewed

Review System Hazards and System-level Safety Constraints (2)

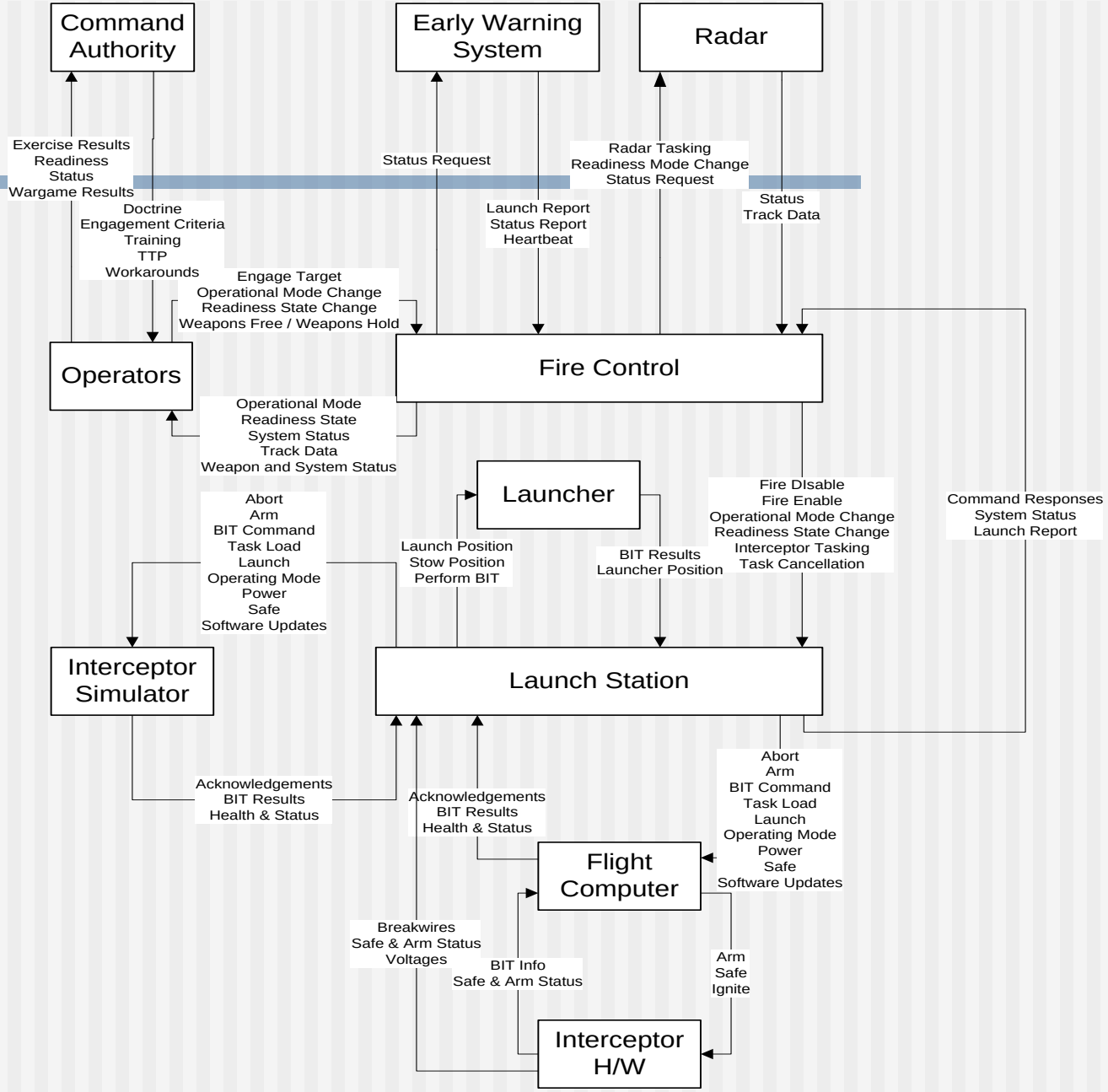
- The hazard being reviewed is:
  - The FMIS system inadvertently launches an interceptor missile
- The top-level system constraints are:
  - *3.7.2. The FMIS system shall make improbable the likelihood of occurrence for catastrophic hazards.*
    - *3.7.2.1 The FMIS system shall make improbable the likelihood of occurrence of inadvertent launch*

SAFEWARE ENGINEERING
Engineering For A Safer World

Define the Safety Control Structure

- Once the hazards to be assessed have been reviewed, the analyst develops a diagram of the safety control structure of the system

SAFEWARE ENGINEERING
Engineering For A Safer World



Safety Control Structure Diagram for FMIS

SAFEWARE ENGINEERING
Engineering For A Safer World

Identify Potentially Inadequate Control Actions

- The next step is to determine how the controlled system can get into a hazardous state
  - A hazardous state is a state that violates the safety constraints defined for the system
- The assessment methodology views hazardous states as a result of ineffective control

SAFEWARE ENGINEERING
Engineering For A Safer World

Identify Potentially Inadequate Control Actions (2)

- Inadequate controls fall into four general categories
  - A required control action is not provided
  - An incorrect or unsafe control action is provided
  - A potentially correct or adequate control action is provided too early, too late, or out of sequence
  - A correct control action is stopped too soon

SAFEWARE ENGINEERING
Engineering For A Safer World

Potential FMIS Inadequate Control Actions

- Fire Enable Missing
  - Fire enable control action directs the launch station (LS) to enable the live fire of interceptors
  - LS will return an error if tasking to interceptor is received prior to Fire Enable
  - If this control missing no launch will occur (Mission Assurance issue)

SAFEWARE ENGINEERING
Engineering For A Safer World

Potential FMIS Inadequate Control Actions (2)

- Fire Enable Provided Incorrectly
  - LS will transition to a state that accepts interceptor tasking and can progress to a launch sequence
  - Combined with other incorrect or mistimed control actions a inadvertent launch can occur

SAFEWARE ENGINEERING
Engineering For A Safer World

Potential FMIS Inadequate Control Actions (3)

- Fire Enable Too Early, Too Late, or Out of Sequence
  - A late fire enable command will only delay the launch station's ability to process a launch sequence, which will not contribute to an inadvertent launch.
  - A fire enable command sent too early could open a window of opportunity for inadvertently progressing toward an inadvertent launch, similar to an incorrect fire enable. The degree of risk this contributes depends both on the likelihood of the inadequate control and how early the control action is carried out.

SAFEWARE ENGINEERING
Engineering For A Safer World

Potential FMIS Inadequate Control Actions (4)

- Fire Enable Too Early, Too Late, or Out of Sequence (cont'd)
  - In the worst case, a fire enable command might be out of sequence with the fire disable command. If possible in the system as designed and built, the system could be left capable of processing interceptor tasking and launching when not intended.

SAFEWARE ENGINEERING
Engineering For A Safer World

Potential FMIS Inadequate Control Actions (5)

- Fire Enable Stopped Too Soon
  - The fire enable command is a single command sent to the launch station to signal that it should allow processing of interceptor tasking. It is not a continuous control like steering a rudder. Therefore, it does not make sense to talk about fire enable in terms of stopping too soon.

SAFEWARE ENGINEERING
Engineering For A Safer World

Determine How Potentially Inadequate Control Action Could Occur

- Look for documentation that the potentially inadequate control action has been designed out of the system, or if present, is adequately mitigated
- The assessment must consider system requirements, design, and verification
- It ensures that appropriate mitigations were:
  - Specified for the system
  - Built into the system
  - Verified to function correctly

Determine How Potentially Inadequate Control Action Could Occur (2)

- During the assessment of the BMDS, this information was summarized on analysis worksheets, adding to the information compiled when identifying potentially inadequate controls

SAFEWARE ENGINEERING
Engineering For A Safer World

FMIS Inadequate Controls

- Fire Enable Provided Incorrectly
  - LS will transition to a state that accepts interceptor tasking and can progress to a launch sequence
  - Combined with other incorrect or mistimed control actions a inadvertent launch can occur.

SAFEWARE ENGINEERING
Engineering For A Safer World

FMIS Inadequate Controls (2)

- Fire Enable Provided Incorrectly (cont'd)
  - The fire control computer is intended to send the fire enable command to the launch station upon receiving a weapons free command from an FMIS operator and while the fire control system has at least one active track
  - the specification requires an "active" track, however, it is difficult to determine what makes a track active
  - The software supports declaring tracks inactive after a certain period with no radar input, after the total predicted impact time for the track, and/or after a confirmed intercept
  - one case was not well considered: if an operator deselects all of these options
  - The inadvertent or intentional entry of a weapons free command would send the fire enable command to the launch station even if there were no threats to engage currently tracked by the system

SAFEWARE ENGINEERING
Engineering For A Safer World

FMIS Inadequate Controls (3)

- Fire Enable Provided Incorrectly (cont'd)
  - The FMIS system undergoes periodic system operability testing using an interceptor simulator that mimics the interceptor flight computer
  - Hazard analysis of the system identified the possibility that commands intended for test activities could be sent to the operational system
  - system status information provided by the LS includes whether the LS is connected only to missile simulators or to any live interceptors
  - If the fire control computer detects a change in this state, it will warn the operator and offer to reset into a matching state
  - there is a small window of time before the LS notifies the fire control component of the change during which the fire control software might send a fire enable command intended for test to the live LS

SAFEWARE ENGINEERING
Engineering For A Safer World

Summary

- In the example, neither of the causal factors identified involved component failures
  - All components were operating exactly as intended
  - Complexity of component interactions led to unanticipated system behavior
  - The problems were discovered using STPA
- STPA also identifies component failures that may cause inadequate control
- Many analysis techniques consider only failure events
  - They ignore the effects of complex system interactions

SAFEWARE ENGINEERING
Engineering For A Safer World

Summary (2)

- The Missile Defense Agency conducted a Non-Advocate Safety Assessment of the Ballistic Missile Defense System using the STPA Methodology
- The STPA safety assessment methodology
  - Provided an orderly, organized way to conduct the analysis
  - Successfully assessed safety risks arising from the integration of the Elements
  - Provided the information necessary to characterize the residual safety risk of hazards associated with the system
  - Provided management a sound basis on which to make risk acceptance decisions
- As changes are made to the system, the differences are assessed by updating the control structure diagrams and assessment analysis templates

SAFEWARE ENGINEERING
Engineering For A Safer World

- For more information contact Safeware Engineering

Grady Lee

443-995-0700

lee@safeware-eng.com

206-328-4880

www.safeware-eng.com

SAFEWARE ENGINEERING
Engineering For A Safer World

The End!!