Applying CAST to behavior-related Product Safety incidents

Mike Hurley

Head of Product Safety,

BAE Systems Electronic Systems Sector

2/20/14

Approved For Public Release

2014 MIT STAMP Workshop 3/26/14

Introduction

- BAE Systems is a global company with a wide variety of Businesses, Products, and Customers

- During development and test of our Products, all incidents, whether an injury is involved or not, provide opportunities for a Learning Organization such as ours to improve the overall level of Product Safety and reduce the probability of such events recurring

- When circumstances of such events do not involve actual failures and thus defy application of traditional root cause analysis methods, the Behavioral approach embodied in CAST has been found to provide insight into causes and solutions for prevention

**This Presentation Will Examine Two Such Events,
The Application Of CAST To Determine Causal Factors,
And How CAST Contributed To Defining Preventive Measures**

Approved For Public Release

CAST: Getting past "blame the operator"

- Its not unusual to see accident investigations stop at the person who was at the controls of the plane when it crashed or who pressed the wrong button just before someone got hurt

- STAMP requires us to look beyond this, to understand why the design of the equipment or the processes & procedures in place defining its assembly, test or use were such that the actions of persons resulted in the accident

- Causal Analysis using Stamp provides a Behavioral approach to causal analysis

"Blame is not an engineering concept"
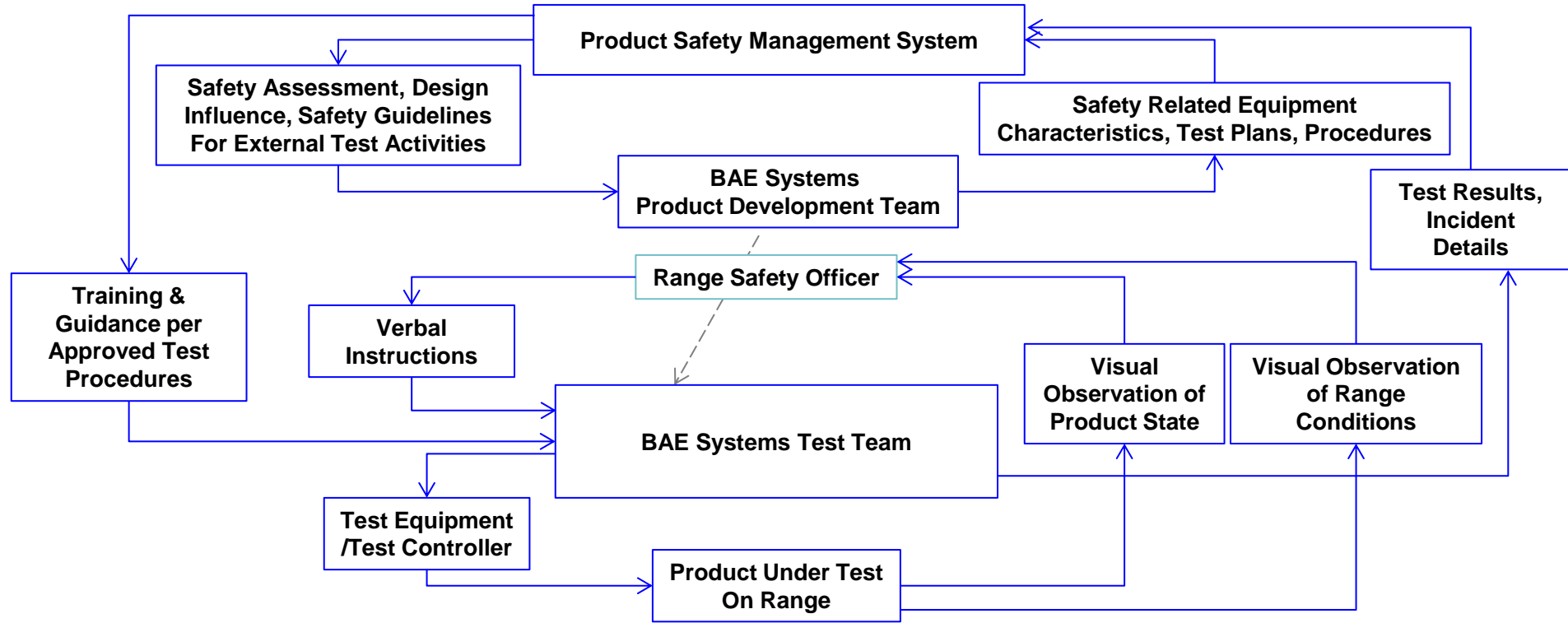
Basic CAST Methodology

- Draw the Control Model

- Identify the Safety Requirements & Constraints – how were these violated?

- Identify Dysfunctional Interactions & Coordination Flaws

  - Inconsistent behavior/actions by personnel indicative that expected behavior was not exhibited or that the system did not respond as expected

  - Evaluate communications/chain of command breakdowns

- Flawed or Inadequate Decisions & Control Actions

  - Personnel engaging in actions that exposed them to the potential hazards

  - Ask whether controls or personnel in charge did not assert sufficient control over the system itself or the actions of persons involved, whether personnel communicate their specific intentions in advance of their actions

- Context: captures the context of what was happening, "where people's minds were", etc.

- Mental Model Flaws – where did people assume or believe things about the system, the controls/constraints, that were incorrect or inaccurate?

Background of the Events

- Both events involved developmental testing of a BAE Systems Product
  - The Product's details are classified, but it can be said that it uses Lithium technology batteries
- A safety assessment had been conducted, potentially hazardous characteristics of expected operation were included in all aspects of test planning and safety training for persons involved in its testing
  - In its natural operation, the release of gases from the batteries, which among other things could affect respiration, is not unusual
  - The Product under test was still in development, therefore other safety hazards such as sufficient heat to ignite proximate flammable objects were known/not unexpected potential events
- In spite of this, and in spite of the fact that nothing in the Product itself failed or performed in any way that had not been expected, both events represented situations that could have resulted in personnel injury through exposure to smoke/gas

FMECAs, Fault Trees Cannot Address These Types Of Events

Approved For Public Release

CAST Control Model In Place Prior To the Events

Product Safety Management System

Safety Assessment, Design Influence, Safety Guidelines For External Test Activities

Safety Related Equipment Characteristics, Test Plans, Procedures

BAE Systems Product Development Team

Test Results, Incident Details

Range Safety Officer

Training & Guidance per Approved Test Procedures

Verbal Instructions

BAE Systems Test Team

Visual Observation of Product State

Visual Observation of Range Conditions

Test Equipment /Test Controller

Product Under Test On Range

Note: the Test Team is a subset of the Development team; during external test activities these persons may be performing a variety of different roles, as participants or observers of the test

Loss To be Avoided Is Harm To The Test Team Or Observers Resulting From Unit Under Test Vent Gas and/or Excessive Heat

Event 1 Details

- Product testing was conducted at a government owned test range

- For safety reasons all personnel (test participants and observers) remained in a bunker until completion of the test sequence and the "all clear" from the Range Safety Officer (non-BAE Systems person) was given verbally

- Multiple BAE Systems personnel then left the bunker and were exposed to drifting smoke with 2 persons exhibiting stomach distress later that evening resulting in reporting of the incident

- Subsequent investigation, including consultation with the BAE Systems staff physician, indicated this was smoke from burning grass, not hazardous fumes, illness was believed food related, minimal vent gas exposure if any (symptoms not consistent with battery vent gas contents which could have caused respiratory distress in some persons)

- Incident was declared not related to any defect or failure in the Product itself, which of course was not the end of the investigation

CAST Analysis: Event 1

- Safety Requirements & Constraints Violated: Personnel must not be exposed to potentially harmful smoke/gas following each Test

- Dysfunctional Interactions & Coordination Flaws
  - one or more personnel present as observers involved themselves in the actual Test/post-Test activity; there was some question as to whether they had all received appropriate training to do so

- Flawed or Inadequate Decisions & Control Actions
  - the person "in charge" of the event did not assert sufficient control over the actions of BAE Systems persons involved after the actual "Test sequence" was completed to prevent potential exposure to any form of smoke/gas

- Context: Personnel involved were enthusiastic and success-oriented, involvement of non-BAE Systems personnel as persons in authority

- Mental Model Flaws
  - BAE Systems personnel assumed a Level of Safety that did not exist
  - Smoke on the range was a "normal" condition to the Range Safety Officer

**Conclusion Drawn: A BAE Systems Person Must be designated As Safety Officer
All BAE Systems Persons Take Direction From Them To Ensure a Common Mental Model**
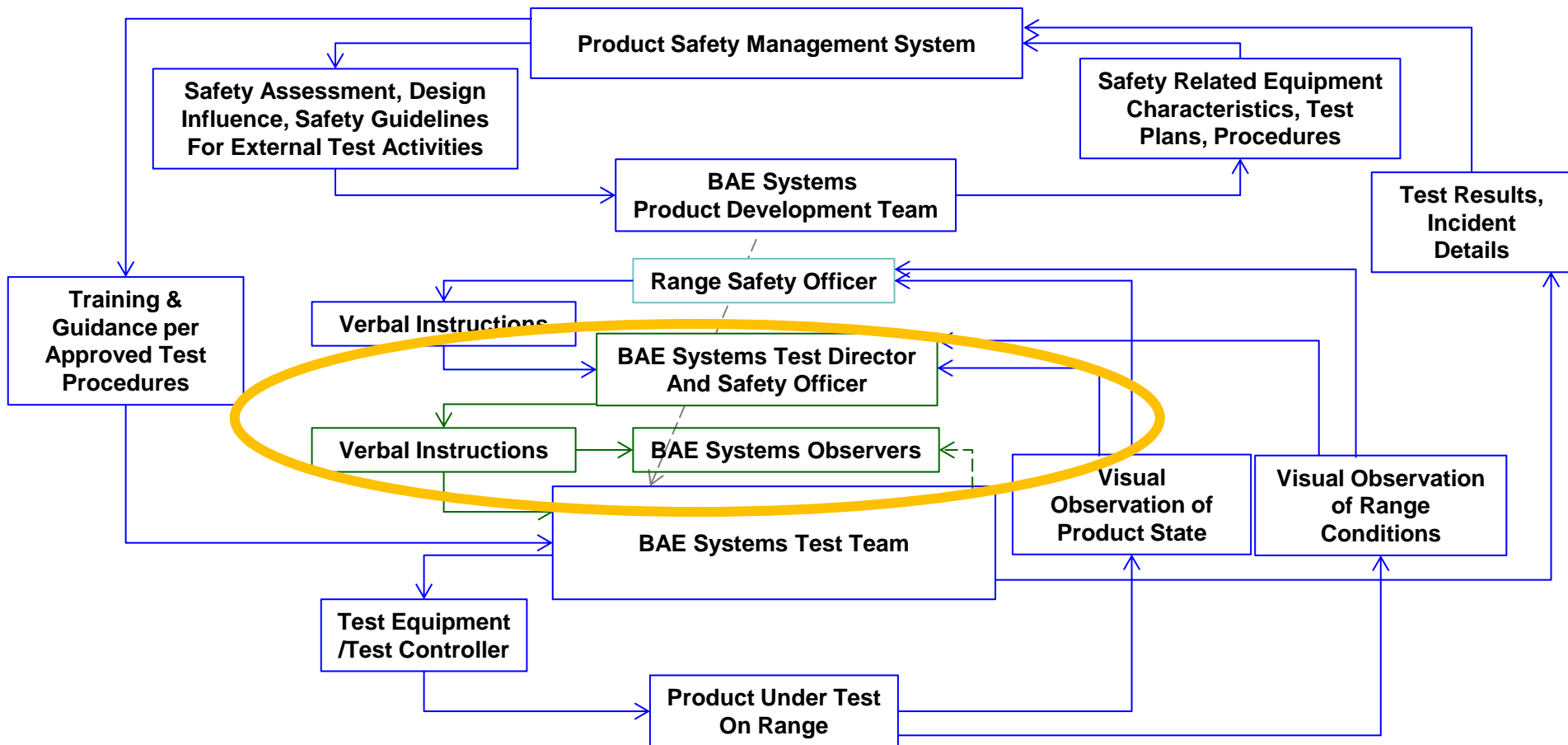
Event 2:

- Product testing was conducted at a subcontractor facility

  - Different test environment than Event 1, some team members were new

- For Safety reasons all personnel (test team and observers) remained at a safe distance until completion of the test sequence and the "all clear" from the Safety Officer (non-BAE Systems person)

- One BAE Systems person there as an observer then approached the unit under test; there was no visible sign that it had vented; they picked it up, turned it around/examining it, and inhaled a small amount of vented gas

  - Fortunately the amount released was not much and the person did not have an underlying respiratory condition thus did not suffer respiratory distress

- Incident was declared not related to any defect or failure in the Product itself, which of course was not the end of the investigation

CAST Analysis: Event 2

- Safety Requirements & Constraints Violated: Personnel must not be exposed to potentially harmful smoke/gas following each Test

- Dysfunctional Interactions & Coordination Flaws
  - the person affected by the event was present as an observer yet involved himself in the actual Test/post-Test activity; there was some question as to whether he had received appropriate training to do so

- Flawed or Inadequate Decisions & Control Actions
  - the person "in charge" of the event did not assert sufficient control over the actions of BAE Systems persons involved after the actual "Test sequence" was completed to prevent potential exposure , nor (it appears) did BAE Systems personnel communicate their specific intentions in advance of their actions

- Context: Personnel involved were enthusiastic and success-oriented, involvement of non-BAE Systems personnel as persons in authority

- Mental Model Flaws: BAE Systems personnel assumed a Level of Safety that did not exist (e.g. absence of signs of a "dramatic" event was assumed to mean no venting had taken place)

Conclusion Drawn: Any persons present as Observers must REMAIN OBSERVERS (You're either IN or OUT in terms of Test Participation – and OUT means OUT)

CAST Control Model With Preventive Measures

Isolate Observers from Exposure to UUT; Ensure a BAE Systems Person Acts As Safety Officer & Directs the Actions of Test Participants

Assessment of CAST Application To This Type Of Events

- Drawing the Control Model helps the analyst think through the "chain of command" but is not as useful in explaining the conclusions/recommendations to Management

- The greatest value was obtained from discussing the events with participants and observers AFTER clarifying this is NOT a "blamestorming" session

  - Dysfunctional Interactions & Coordination Flaws: often some personnel will recall observed inconsistent behavior/actions and communication breakdowns on the parts of others (though usually not their own)

  - Flawed or Inadequate Decisions & Control Actions can be revealed by walking through what should have happened with those who were present who can then identify where things went off the intended path and sometimes why

  - Ditto for identifying Context as in, "where people's minds were", etc.

- Arriving at Mental Model Flaws – where did people assume or believe things about the system, the controls/constraints, that were incorrect or inaccurate – then requires the Analyst to step back and review the inputs collected and visualize the events from the different perspectives of participants, observers, authority figures.

  - Example - why would the RSO give the all clear while smoke was still drifting across the range unless to him it was a normal condition?

Conclusions

- This presentation has shown how the application of CAST to these events:

  - Enabled derivation of preventive action that was behavior-focused, and that was readily translated into guidance for external tests/demonstrations to prevent recurrence of this type of near-miss

  - Captured the results of the analysis in a format that was easier to present and explain to management than traditional analytical method outputs

  - Created a context for explaining the benefits from the resulting preventive actions that was readily understood by management and the members of the team

As Systems Have Become More Autonomous We Are Seeing An Increase In Events For Which Traditional Tools Cannot Serve Us Due To The Underlying Behavioral Causes

Approved For Public Release

2014 MIT STAMP Workshop 3/26/14