# From CAST to STPA – Closing the loop

Presented By
Mark Monroe
Product Safety Engineer,
BAE Systems Electronic Systems Sector
3/27/15


Prepared by Mark Monroe, Mike Hurley; BAE Systems Inc.

BAE SYSTEMS
INSPIRED WORK

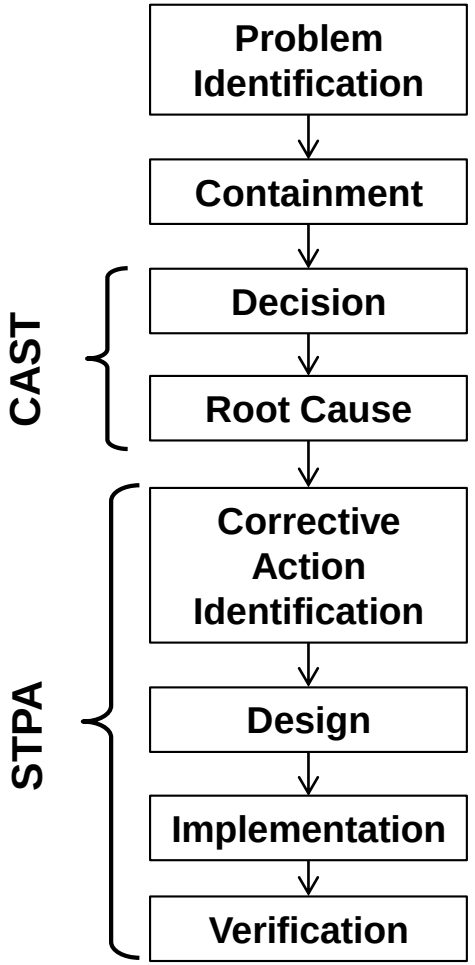
# Introduction

- BAE Systems is a global company with a wide variety of Businesses, Products, and Customers
- During development and test of our Products, all incidents and injuries, no matter how minor, 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 STPA to identify solutions for prevention
- BAE Systems has been utilizing this process to analyze not only injuries/incidents and near misses, but potential areas of concern also.

**This Presentation Will Examine One Such Event,**
**The Application Of CAST To Determine Causal Factors,**
**And How STPA Contributed To Identify Multiple Corrective Action Options**

# Sequence for success

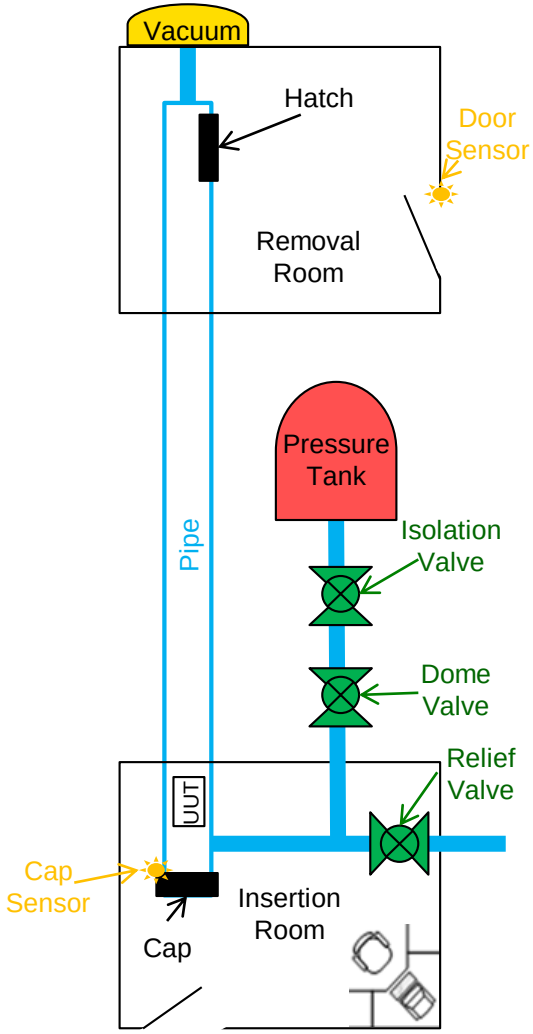
- Initial investigation performed using traditional means.
- Initial update was performed to the Software to contain the problem.
- It was decided to revise the control Software to raise the entire Level of Safety of the facility.
- Created CAST Model to identify root cause of event.
- Utilized STPA to translate the results of the model to actionable improvements.
- Drew a state diagram from the STPA so Software could incorporate it into their plans and provide verification methods.
- Implement Software.
- Verify Software



BAE SYSTEMS
INSPIRED WORK

# Background: pneumatic test facility

- The test facility consists of a long pipe between two rooms through which a Unit Under Test (UUT) is forced using highly pressurized air. The air is provided by a compressor and storage tank with various valves (Pressure Isolation Valve, Dome Valve, Vent Valve) between the compressor and the tank, the tank and the pipe, and the tank and a venting pipe.
- The UUT is loaded at one end of the pipe through a cap which has a magnetic switch attached so the controlling software can detect whether the cap is closed or not. The PC with the control software is located in this room (insertion room).
- The other end of the pipe has a removable hatch section that allows the UUT to be removed. There is no sensor on the hatch but there is a sensor on the door to the area which the software can use to detect when the door is opened.
- Another sequence is used if the UUT has not reached the end, which can draw a vacuum in front of the UUT and put pressurized air behind it.
- The Vent valve is intended to release system pressure safely outside the facility when the normal test sequence is aborted.



BAE SYSTEMS
INSPIRED WORK

# Incident details

- Following a Test, a UUT removal sequence was commanded by the operator (combination of vacuum and pressurized air in the pipe) which is applied to move the UUT all the way to the removal room hatch for extraction.
- An employee entered the removal room before the UUT removal sequence was completed; by opening the door, he interrupted the sequence which caused the software to close both the Pressure Isolation Valve and the Dome Valve. The employee removed the UUT, replaced the pipe access hatch, and closed the removal room door, re-engaging the magnetic switch on the door.
- A second employee was preparing for the next test event and removed the cap in the insertion room (opening that sensor) to load another UUT.
- The second employee attempted to reattach the Cap; as soon as the software detected closure of the cap sensor, the suspended UUT removal sequence resumed by opening the “Dome Valve” which allowed high pressure air (trapped between the Dome Valve and the Pressure Isolation Valve) to enter the pipe.
- The partially closed cap was expelled, injuring the employee’s thumb.
  - Employee received medical attention and was cleared to return to work
- **No actual failure was involved and everything worked as designed, though not as intended.**

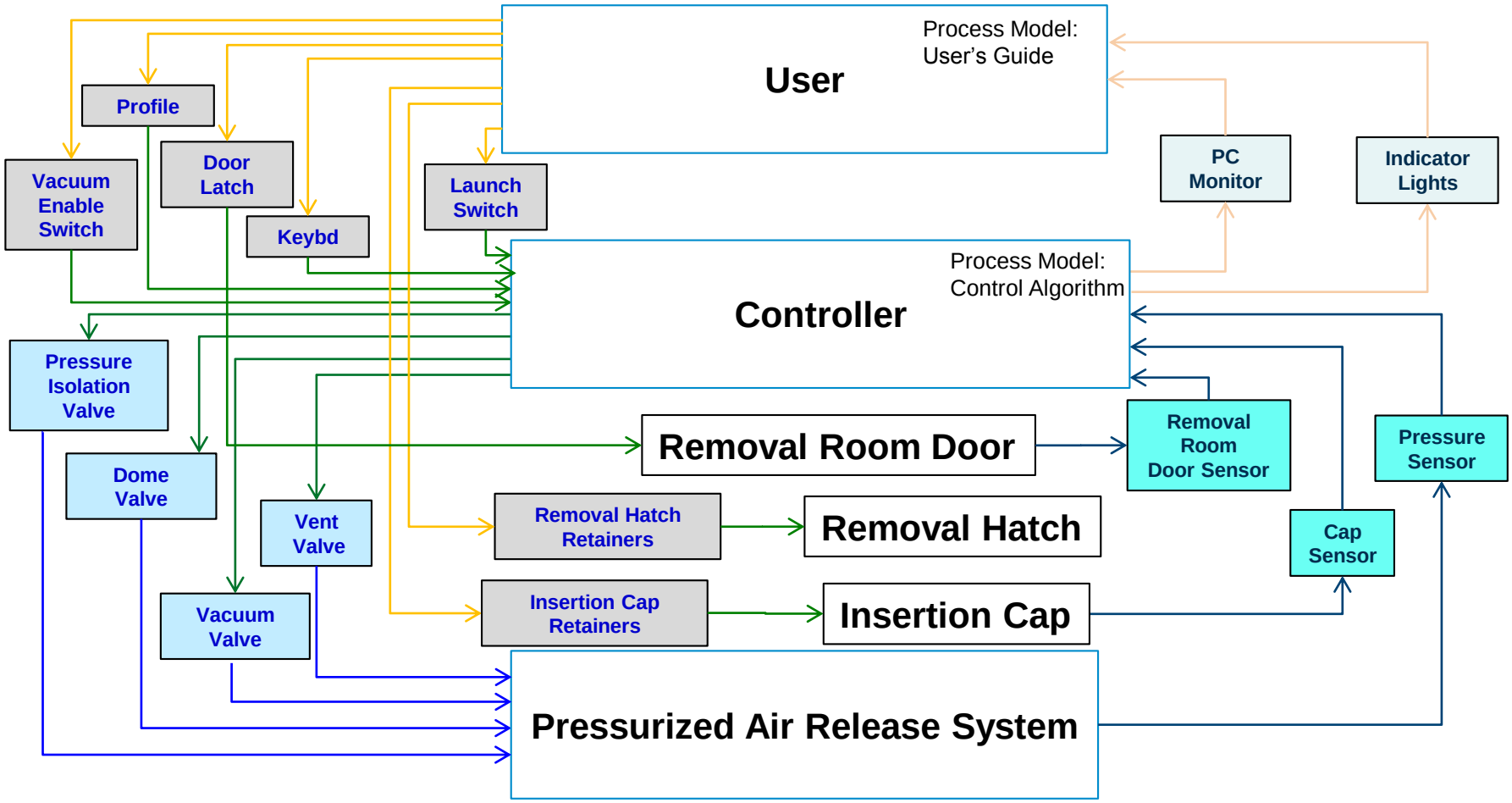
BAE SYSTEMS
INSPIRED WORK

# Traditional investigation

- The intended operation is that the system shall enter the **SAFE state** when the removal event is complete, the cap is removed and replaced or the removal room door is opened and closed.
- High Pressure Air must not be allowed to enter the pipe under any conditions that present possibility of injury to personnel
  - When the insertion Cap is not secured in place
  - When the removal Hatch is not secured in place
- An Engineering Analysis of the software revealed that the removal routine was flawed and the operating event that injured the Operator was duplicated.
- Opening of the removal room door introduced a Safe state for that area only.
- At the completion of the removal routine the pressure valves were only “closed” leaving residual pressure in the system. No SAFE state was ever entered.
- The following software improvements were made
  - Vent the pressurized tank if the specified removal sequence is not followed e.g. if a sensor opens mid-sequence
  - An additional hardware control (Emergency Switch Reactivation) following such interruptions that requires the operator to initiate resumption of operation (re-pressurize the tank)
- **It was also decided to raise the overall level of Safety for the facility.**

# Application of CAST

## Control Model



BAE SYSTEMS
INSPIRED WORK

# Application of CAST

- Further review of the software revealed an unanticipated unsafe condition
  - Entering the launch sequence with the system awaiting a trigger event from the operator any attempt to command a SAFE state incurred a 10 second wait state instead of a shutdown.
- Safety Requirements & Constraints Violated:
  - High Pressure Air must not be allowed to enter the pipe under any conditions that present possibility of injury to personnel
  - Injury could arise from multiple scenarios involving Cap not secured, persons in removal Room in proximity of the hatch while it is opened/not secured to the pipe
- Dysfunctional Interactions & Coordination Flaws
  - The injured employee believed the system was in a safe state and would remain there until he took action to change it (e.g. believed reattachment of the cap would not degrade system Safety)
- Flawed or Inadequate Decisions & Control Actions
  - The Safety constraints that existed in the software did not anticipate this sequence of events; the software caused the removal sequence to resume based on closure of the cap sensor (which is possible without the cap actually being secured to the pipe) and did not require some action on the part of the operator following interruption of the removal sequence before resuming it
- Context:
  - Personnel enthusiastic and success-oriented
- Mental Model Flaws
  - Personnel assumed a Level of Safety that did not exist

BAE SYSTEMS
INSPIRED WORK

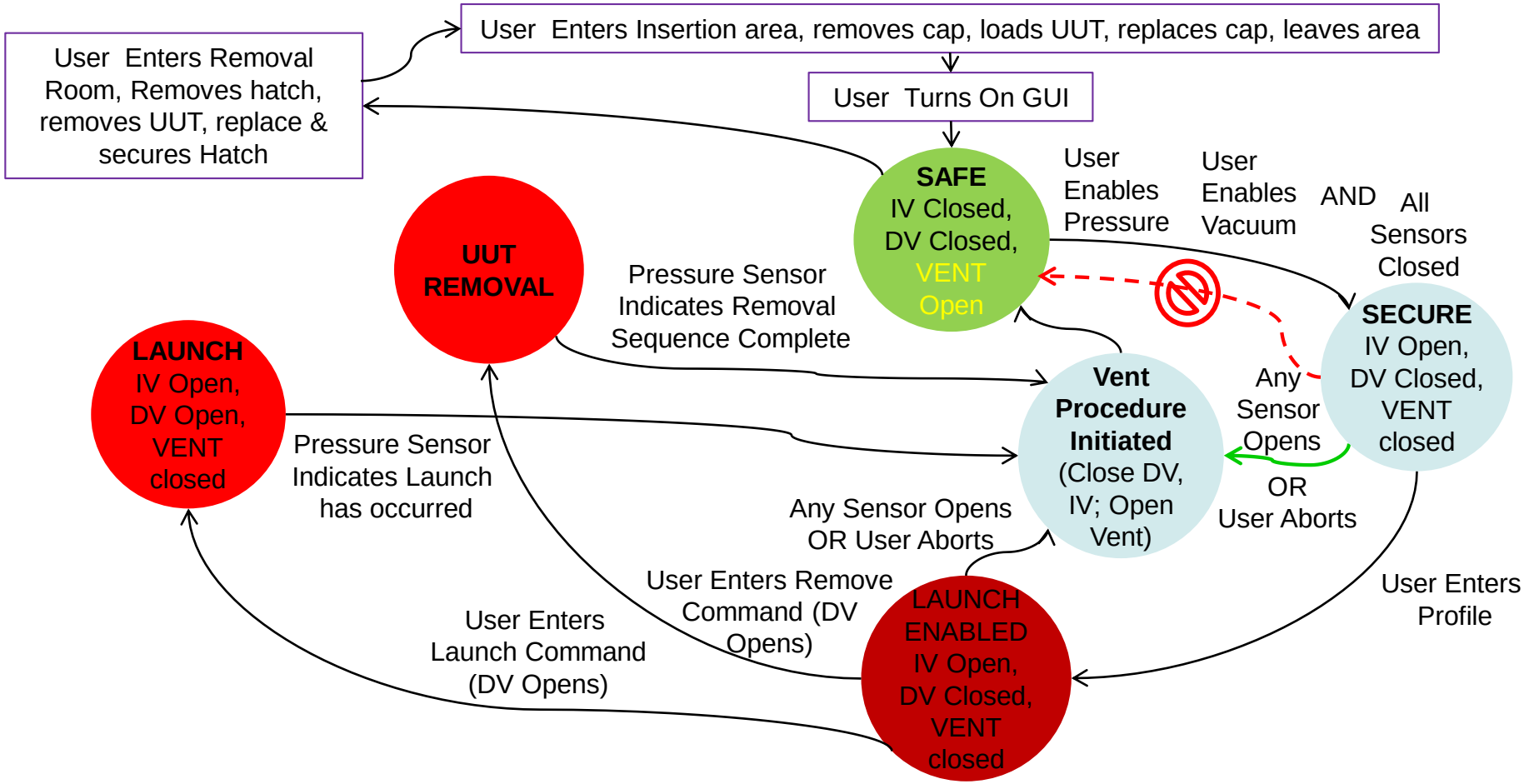
# STPA

Unsafe Context: Door is not latched and user is near it

| Potentially Unsafe Command | Not Provided | Provided | Too Early | Too Late | Wrong Sequence | Stopped Too Soon | Applied Too Long |
|---|---|---|---|---|---|---|---|
| Release pressure into the pipe (Isolation Valve or Dome Valve Open and Vent Closed) | Launch or removal routine cannot be completed | Pressure In Pipe when the Cap is not secured | Pressure In Pipe before the Cap is secured | No Effect | Pressure In Pipe after the Cap is opened for loading | Controller removes pressure before the Launch has completed | Pressure in the pipe after the launch sequence completed AND Operator attempts to remove Cap |
| **Cause(s):** | Operator fails to secure Cap AND Pressure Sensor fails AND Isolation Valve or Dome Valve Open AND Vent closed | | | | Operator opens Cap while pressure remains in pipe | | Isolation Valve or Dome Valve fail stuck open, Vent fails stuck closed |
| **Preventive Measures** | Disable sequence & transition to SAFE State if cap not secured AND operator is in vicinity | | | | Disable sequence & transition to SAFE State if cap not secured AND operator is in vicinity if pressure is in the pipe after normal sequence completed | | |

**Ultimate answer: To prevent system from entering Safe State with pressure trapped between valves in pipe, all states must enter SAFE state through Venting state.**

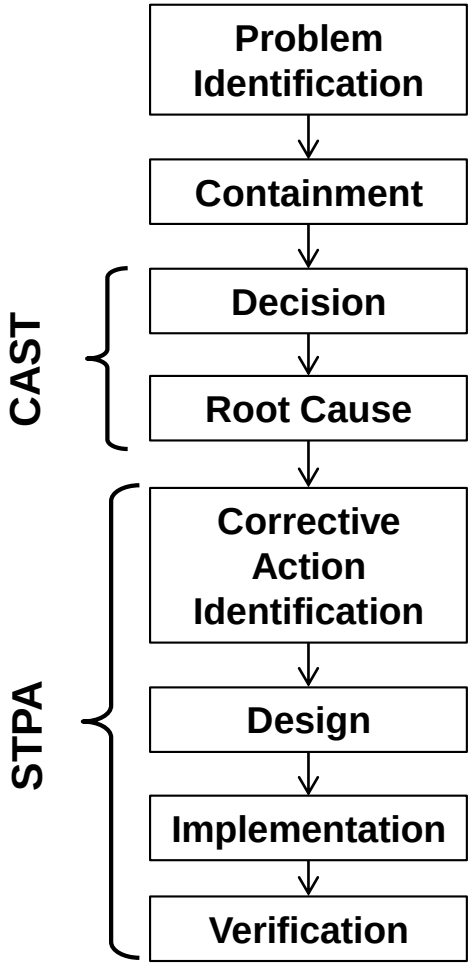
# State diagram




**State Diagram used to translate STPA for Software Team Regression Tests**
**Shows all states must transition through Vent to get to SAFE State**

# Status / next steps

- Problem Identified
- Containment Completed - Initial incident corrected
- Root Cause Assessment Completed – CAST utilized
- Corrective Action Approved – STPA used to identify method for Long term improvement in the level of Safety for the entire facility
- Software Design Updated – STPA converted to State Diagram for translation to Software
- Final Software Release in Process
- Regression Testing Underway



# Conclusions

- This presentation has shown how the combined application of CAST and STPA has improved overall facility Safety.
- The sequence of applying CAST to fully understand the causality of a hazardous event, then applying STPA to the Control Diagram identifies the potentially unsafe commands.