Knowing When to Stop:
An Examination of Methods to Minimize the False Negative Risk of Automated Abort Triggers

RAM XI Training Summit

October 2018

Patrick Fussell, QD35, Bastion Technologies, Inc.

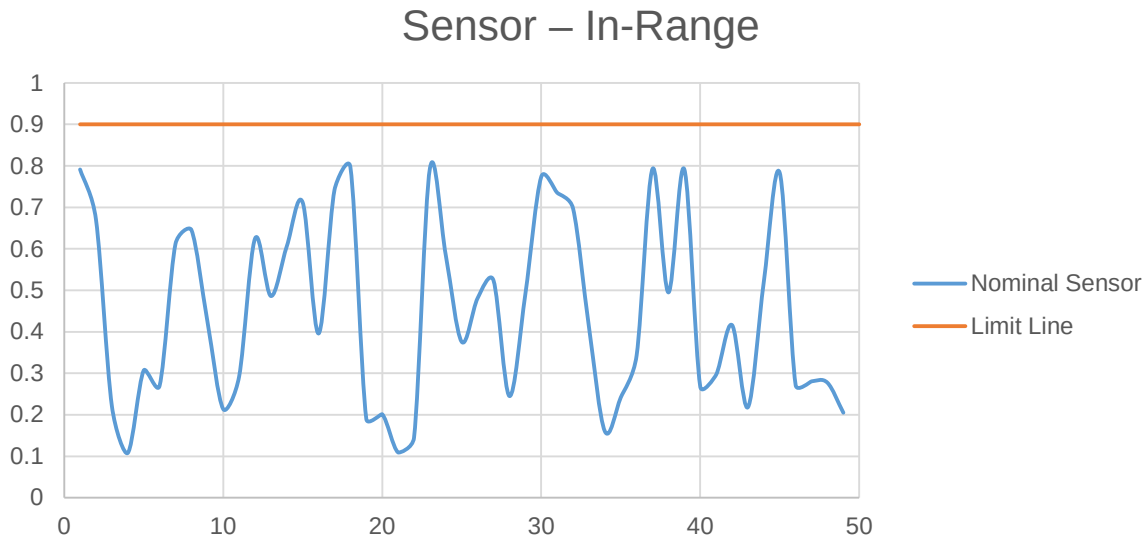
Esha Rahaman, QD35, Bastion Technologies, Inc.

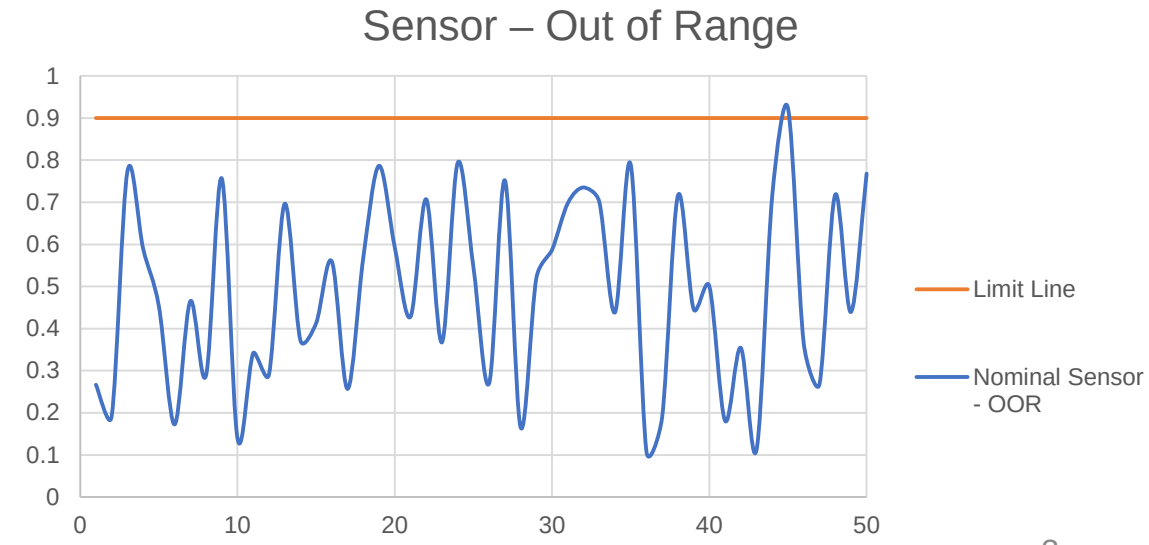
Introduction

- Crewed launch vehicles contain a series of abort options
- Ground Control and Range Safety are able to manual initiate aborts and the flight safety system
- However, due to the very fast response time required to ensure safety of the crew in many abort scenarios, the flight computers are able to initiate automatic aborts
- An automated abort will safe the vehicle by cutting off the engines, get the crew capsule away from the vehicle, and if necessary activate the flight safety system

Automated Aborts

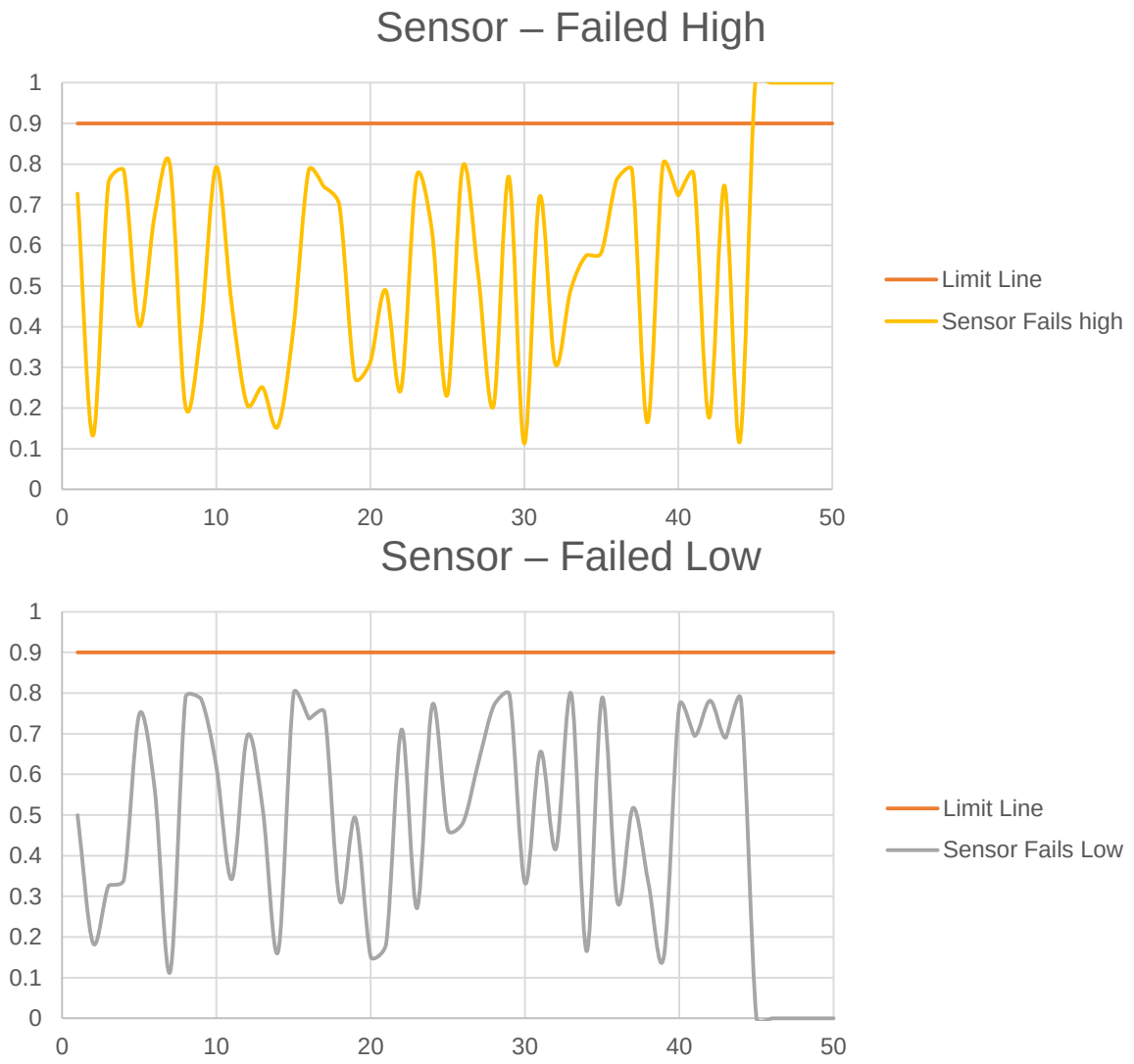
- Flight computers monitor sensor data to determine if abort actions should be initiated based on current flight conditions
- These range from simply warnings to immediately aborting and initiating the flight safety system
- Failure to identify an out of range condition it is considered a false negative failure
- If the flight computer takes an abort action when conditions are nominal it is considered a false positive failure





Sensor Failure Modes

- Sensor failure modes include ‘fail high’ and ‘fail low’
- Fail High - upon failure the signal will be at the upper range
- Fail Low - upon failure the signal be at the lower range
- Either sensor failure can potentially lead to a false positive OR a false negative failure depending on the limits for that parameter



Sensor False Negative Mitigation

- To protect against false negative failures a variety of methods are used
  - Sensor Redundancy
  - Sensor failure logic resiliency
  - Sensors for multiple independent flight conditions
- Unfortunately, most of these will inadvertently increase the false positive risk
- This presentation will review PRA analysis of several common methods to mitigate false negative risks and present sensitivities showing how the methods affect false negative and positive risks

Additional Considerations

- Software used to interpret the signals will be modified when using any of these methodologies
  - This increase in complexity, will in turn decrease software reliability

- This can be a driver in decreasing over-all reliability when you are trying to mitigate it

Quantitative Analysis Using Notional Sensor Hardware

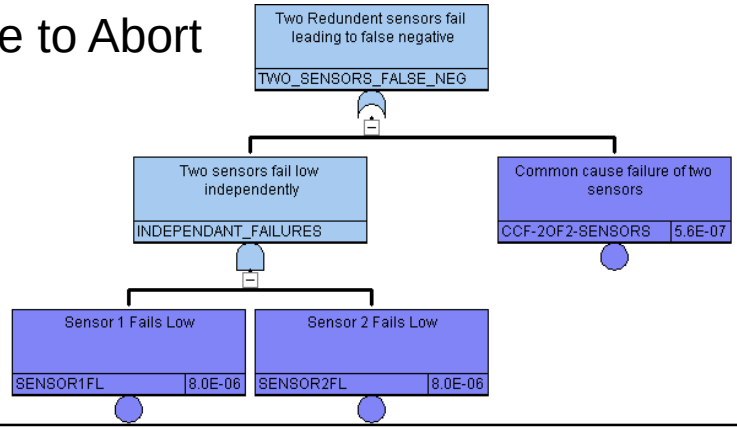
- In the following examples we will be looking at two kinds of sensors
  - The first has a failure mode distribution of 15% Fails High, and 85% Fails Low with a reliability of 0.99999
  - The second sensor has a failure mode evenly split with a reliability of 0.999995
  - These are notional, but realistic failure probabilities
- A false negative will be defined as a failed low signal from all sensors
  - In our examples this would cause a failure to abort when the situation would require an abort
- A false positive will be defined as any failed high sensor
  - In our example this causes a spurious abort

Sensor Redundancy

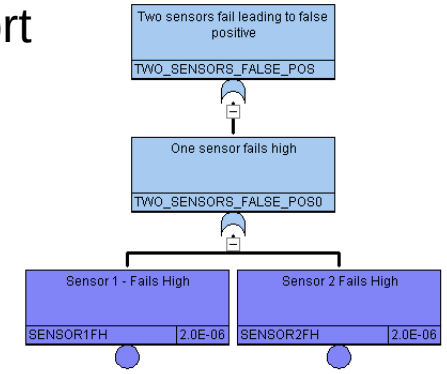
Scenario	Fails to Abort	Spurious Abort	Total	Total+SW
One Sensor	1 in 120,000	1 in 670,000	1 in 100,000	1 in 91,000
Two Sensors	1 in 1,700,000	1 in 330,000	1 in 280,000	1 in 210,000

- Adding another sensor reduces the false negative risk exposure
- This however increases exposure to false positive failures
- Depending on the sensor configuration's failure mode distribution this can end up leading to a higher over-all loss of mission risk
- Increase in software complexity decreases software reliability
- False negative is not lowered as much as may be expected due to Common Cause

Failure to Abort



Spurious Abort

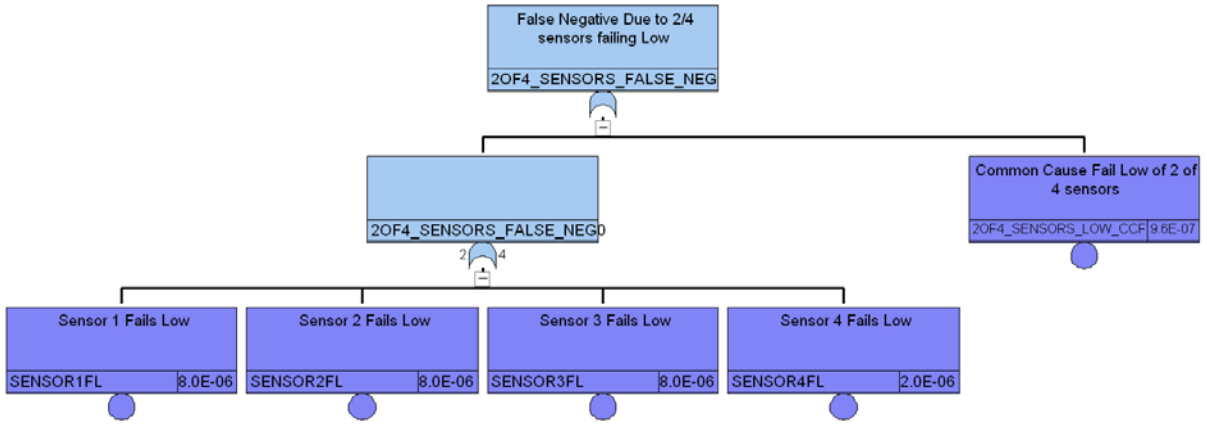


Sensor Failure Logic Resiliency

Scenario	Fails to Abort	Spurious Abort	Total	Total+SW
One Sensor	1 in 120,000	1 in 670,000	1 in 100,000	1 in 91,000
3/4 Sensor logic	1 in 980,000	1 in 5,600,000	1 in 830,000	1 in 310,000

- Adding a three of four required sensor logic reduces both false negative and positive
- This will again decrease software reliability, but generally not enough to outweigh the benefits
- While this lowers the overall risk, it also increases flight sensor hardware, and may not be feasible when modifying a current design due to cost and schedule constraints

Failure to Abort



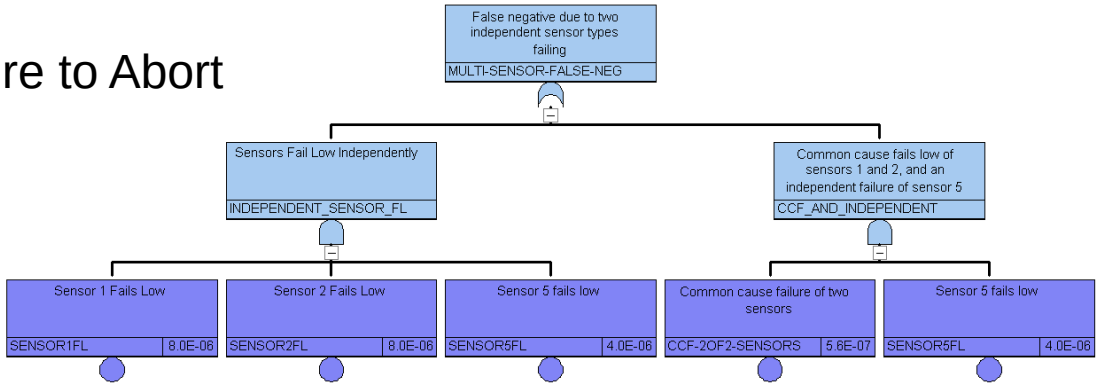
Spurious Abort logic will be identical, but with fails high.

Applying Independent Sensor Check

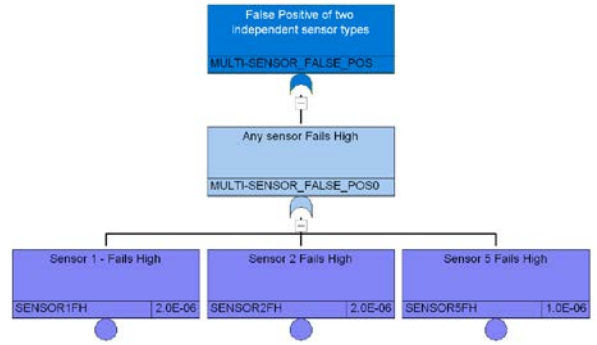
Scenario	Fails to Abort	Spurious Abort	Total	Total+SW
One Sensor	1 in 120,000	1 in 670,000	1 in 100,000	1 in 91,000
Independent Sensor added	< 1 in 1,000,000,000	1 in 250,000	1 in 250,000	1 in 190,000

- Using multiple parameters, such as temperature and pressure to self check
  - 3/3 low signals leads to a false negative
  - 1/3 high signals triggers the abort
- Essentially reduces all risk due to a false negative, due to independent sensor failure allowing common cause to be less of an issue
- Adds significant software complexity, decreasing reliability of software

Failure to Abort



Spurious Abort



Design Change

Scenario	Fails to Abort	Spurious Abort	Total	Total+SW
Two Sensors	1 in 1,700,000	1 in 330,000	1 in 280,000	1 in 210,000
Independent Sensor added	1 in 250,000	< 1 in 1,000,000,000	1 in 250,000	1 in 190,000

- In a hypothetical design change, a redundant sensor design was found to be too susceptible to false positive failure, driven by common cause failures
- This leads to an effort to redesign the sensors to make use of an independent sensor already available
- The change will essentially remove the chance of a false negative failure
- However, due to the software changes required and the additional risk of false positive from the added sensor, PRA results show that the change will lead to an overall decrease in reliability

Summary /Conclusion

- The failure of sensors used in automatic aborts can lead to two very different failure scenarios based on the failure mode
- Components, such as sensors, that have multiple failure modes and effects, can lead to unintentional risk increases if design changes are focused on improving only one of these effects.
- When performing a design change, risk-based analysis with a PRA model is a critical input for risk-based decision making
- This gives decision makers a full picture of the risk that will be incurred/removed from the system based on the proposed change
- When analyzing sensors, or any component with varying failure modes and effects, using a fully integrated system model to ensure all risk changes are captured is vital
- The best option reliability wise is resiliency using a voting logic. This has a higher reliability for both failure modes. Cost, vehicle weight, and schedule often require a compromise, using a PRA in tandem with design will help balance risk vs. costs