Mitigating the June 2007 International Space Station (ISS) Russian Segment Computer Anomaly in your Design

Project Management Challenge 2008

Daytona Beach, Florida

February 26 - 27, 2008

Mitchell Davis

NASA Technical Fellow for Avionics

NASA Engineering & Safety Center

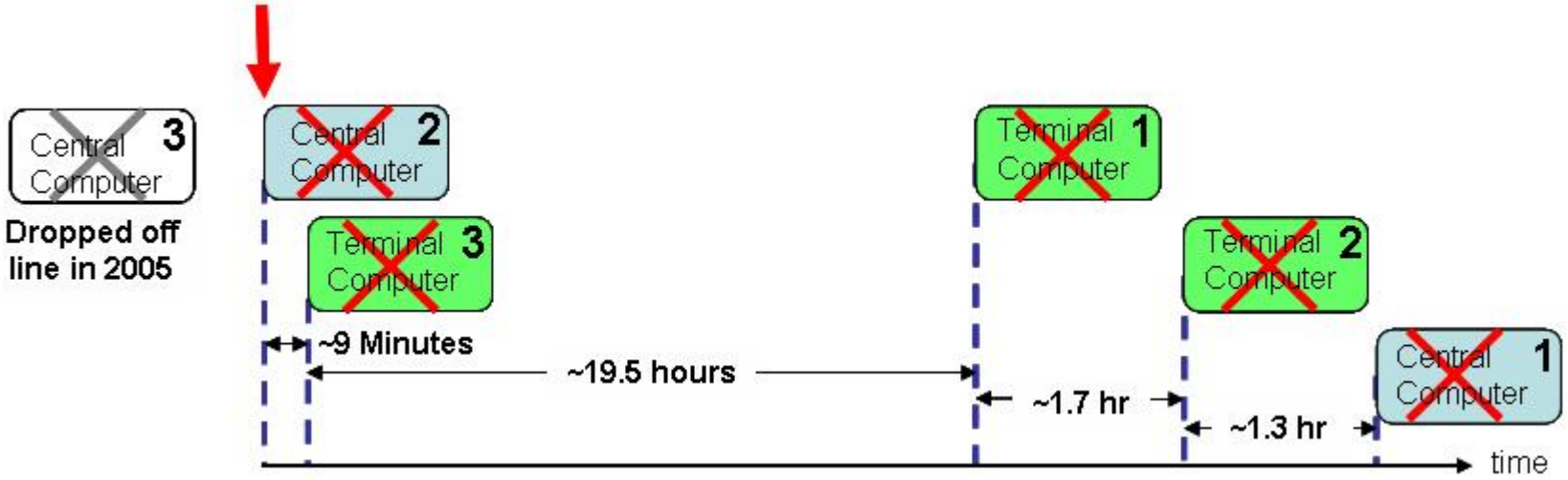
Summary

Purpose: This presentation considers the resulting design features on the ISS computers and redundancy implementation in relationship to the June 2007 ISS computer shutdown anomaly.

- The resulting design features dictate how each subsystem responds to particular fault, which in turn dictates the entire system response.
- The first section covers the anomaly and recovery
- The second sections covers the lower level implementation details in connection to the threat
- This paper in intended to provide an example of the design decisions covered in earlier NESC “risk-based design” presentations.

Anomaly Timeline

- In June 2007, during ISS Assembly Mission 13A (STS-117) on day 3 of a 11 day mission at 20:41:44 of GMT day 162, the first Russian Segment (RS) Service Module (SM) Central Computer-2 went off-line.
  - Central Computer-3 had not been part of the active set since 2005
- An RS Terminal computer went off line minutes later and within 24 hours all 6 RS control computers were non-functional.
- Repeated attempts to bring the computers back to an operational state over the next three days produced only temporary and erratic results.

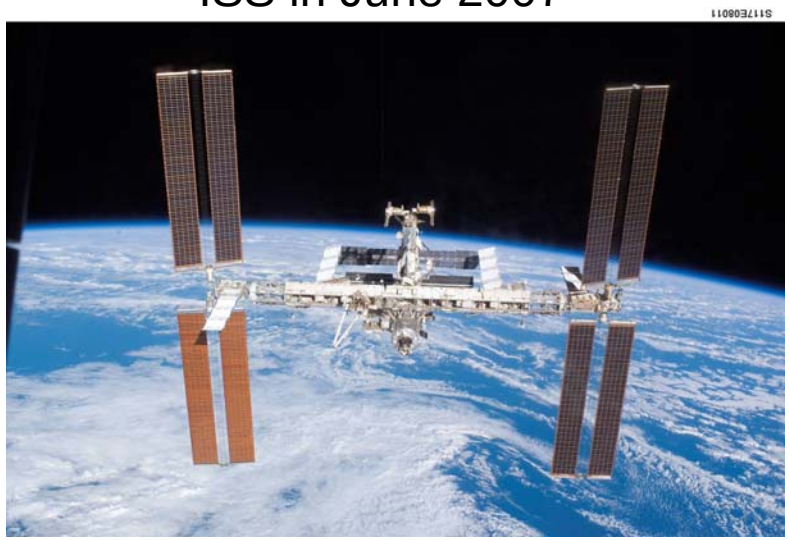


ISS/Shuttle Impact

- The loss of the RS computers resulted in the inability to remotely control some Russian systems and for the ISS to resume attitude control of the mated vehicle configuration.

- Orbiter provided critical independent attitude control of the combined ISS/shuttle allowing opportunity and time to restore ISS system.

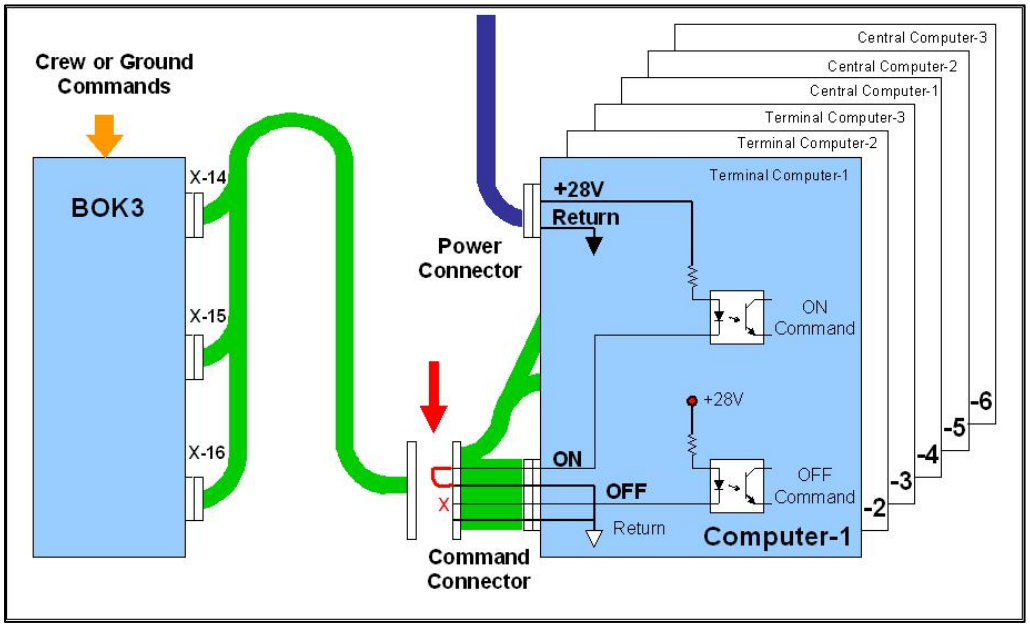
ISS in June 2007



- The ISS attitude control and redundancy strategy relies on both the US and Russian Segment attitude control systems.
  - The normal method of ISS attitude control is non-propulsive via the four US Control Moment Gyroscopes (CMGs).
  - The CMGs have limited torque output, therefore Russian propulsive control (requiring RS computers) is used to maneuver the ISS or if the CMGs were to saturate due to some significant attitude disturbance.

Temporary Mitigation

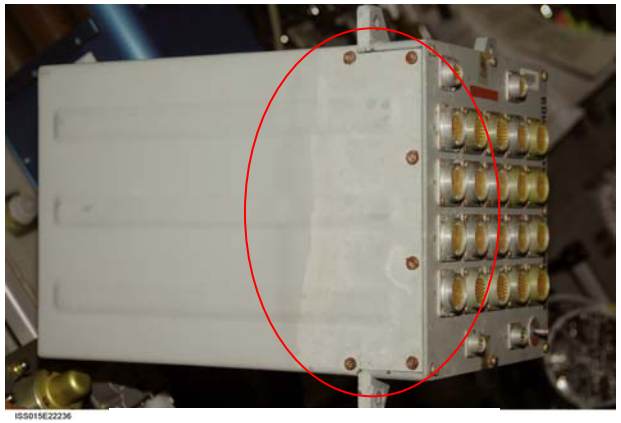
- The are multiple RS computers for redundancy and they could be configured by ON/OFF command signals on an “as needed” but intended infrequent basis.
- The ON/OFF commands can come from either the crew or ground control and are routed to the computers by the BOK3.



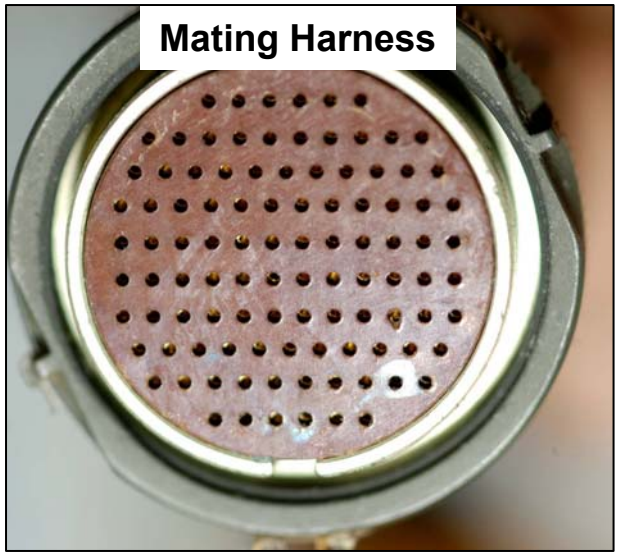
- After three days of erratic computer operation, the harnesses between the BOK3 command unit and the computers were disconnected
  - Thus removing any shorting connection on the BOK3 side of the interface harness.
  - Shorting jumpers provided a continuous ON command into the computers’ pulse command input.

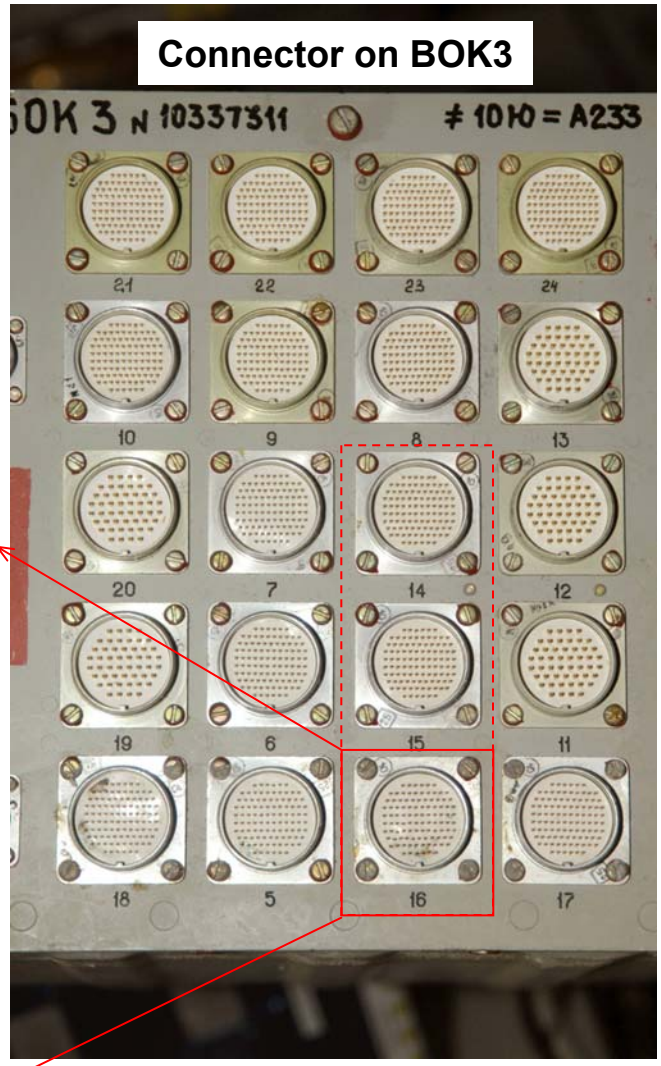
BOK3 & Harness Photographs

Corrosion/contamination found on BOK3 command box and associated harness



BOK3 Discoloration

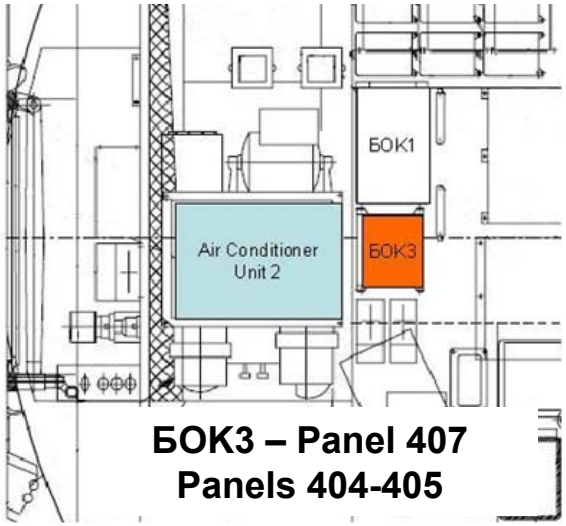




Moisture & Condensation

- The ISS has a requirement for no condensation in the pressurized environment and historically, the ISS vehicle has been very dry with no reports of condensation by the crew.

- Both the US and Russian segments have condensing heat exchangers as part of their air conditioning systems. The condensed water is recycled only by the Russian environmental control system because the US water recycling system is not yet operational.



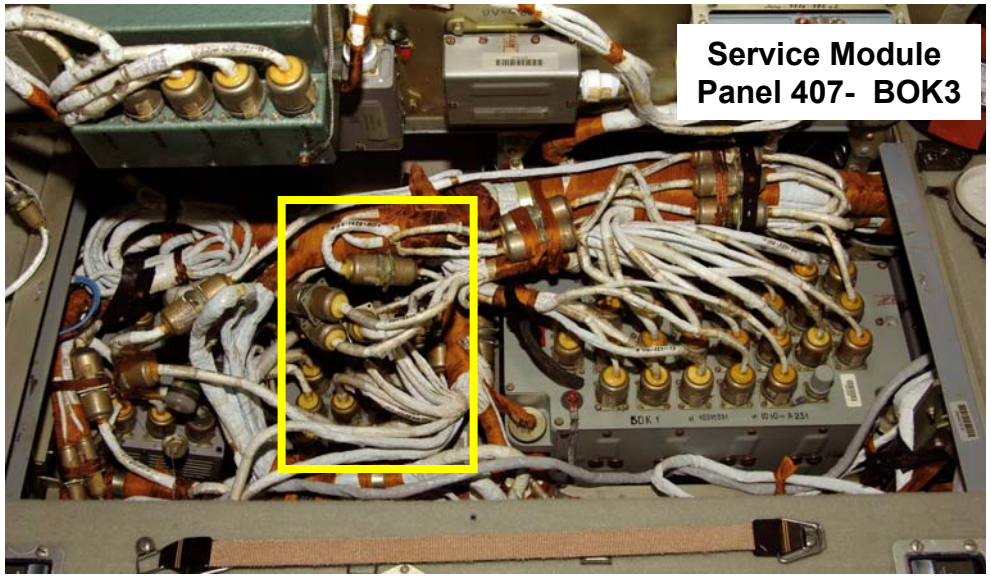
- The air conditioner and the BOK3 are adjacent to each other.

- Factors that influence the amount of condensation include:
  - There have been momentary periods where debris blocking the outlet line and membrane water separator resulted in a raised dew point.
  - During Space Shuttle docking, the ISS crew size increase to a maximum of 10 people can significantly increases the atmospheric moisture.

- In spite of requirements, constraints and operational considerations, influences outside beyond control can lead to momentarily undesirable environments.

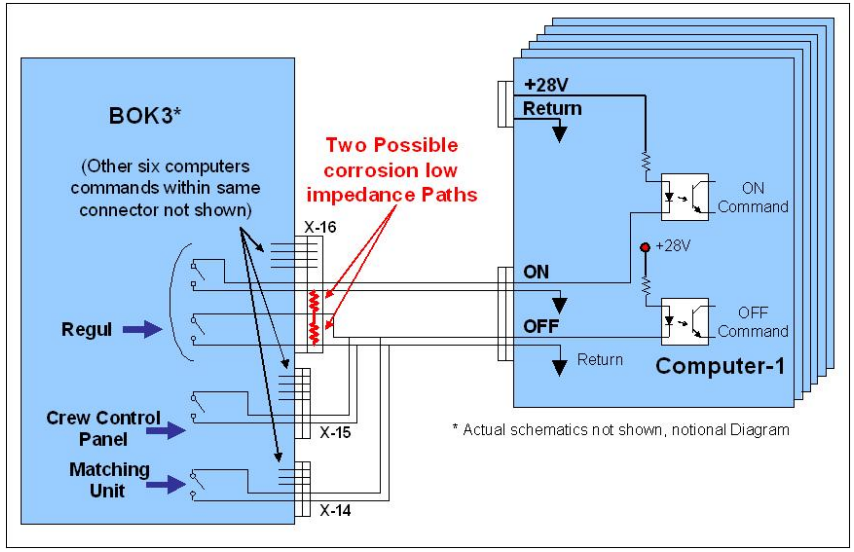
Cause and Correction

- Temporary circuit jumpers remained in place until ISS mission 13A.1 (STS-118)
- Mission 13A.1 included a new BOK3, connectors and harness
- Operational changes were put in place to be better prepared for a similar event
  - Method was developed to allow attitude control handovers from Shuttle directly to CMG control (without the need for Russian Thrusters) This was demonstrated during a subsequent assembly flight.
  - Periodic inspections of RS interior compartments were instituted to look for moisture



BOK3 to Computer ON/OFF Commands

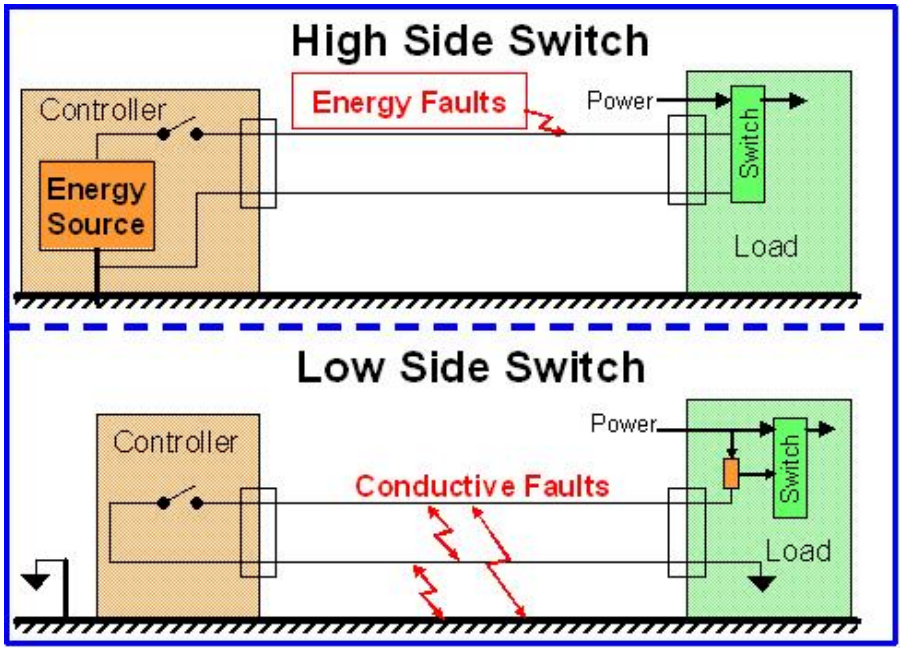
- The BOK3 receives three command inputs (Regul, Crew Control Panel & the matching unit) and outputs the appropriate ON & OFF commands to the six individual computers.
- Commanding implementation in the BOK3 is by providing a low impedance path between the two computer provide connections, (common called "Low Side" switching.)



- The three connectors (X-14, X-15, & X-16) contain 24 wires in which half are common returns available to complete the circuit.
- Spice circuit modeling indicated that a kilo-ohm range resistive path between the command and any return was sufficient current to active the opto-coupler.
- The Russian system is unique in that the primary power is isolated from chassis by several 100kohm therefore conductive paths to chassis would not activate the command.

“Low-side” Switching & Threats

Typical Grounding Configuration



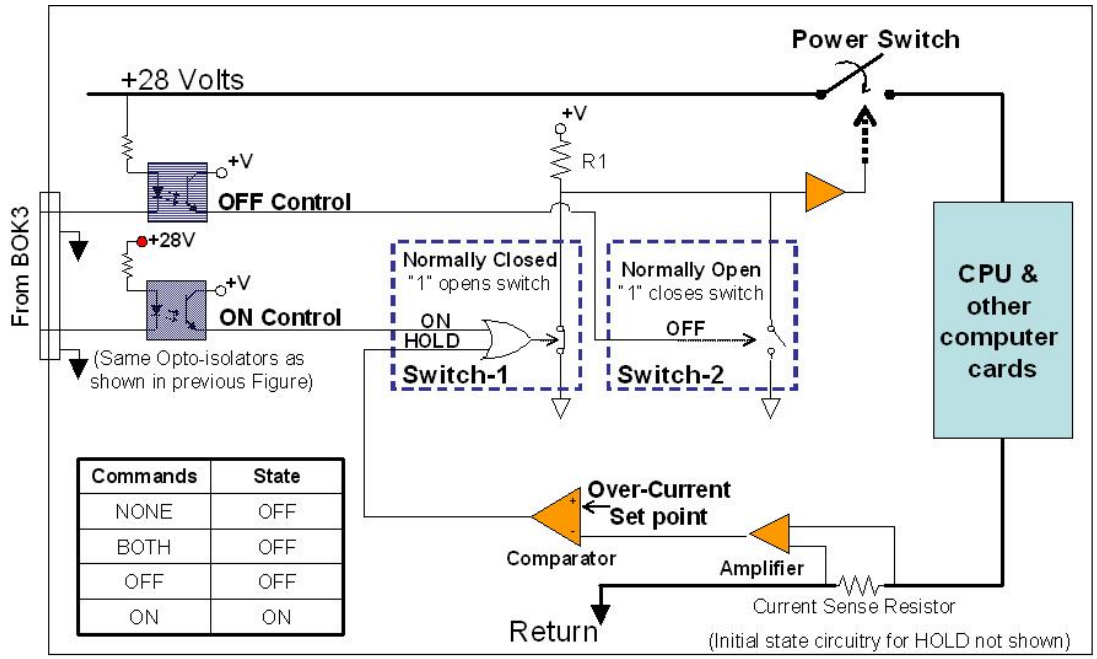
- Key factors that determine the degree of threat include the *interaction of* circuit design, system ground configuration and credible faults.
- The two configurations have different probability of occurrences to inadvertent commanding faults and roughly equal no-command faults
- The inadvertent command threats to the “high-side” switch configuration include energy sources with sufficient voltage, current and time duration as well as a conductive path to the command circuit.
- The inadvertent command threats to the “Low-side” switch configuration include conductive paths between the command circuit and signal return or chassis.
- The same approach applies to addressing failure modes of the lower level command circuit as well as higher levels within the architecture.

Computer Block Diagram

- Power to the computer circuitry is controlled by a series of stages and the Power Switch closes when both switch-1 and switch-2 are open.

- With both ON and OFF commands present, the OFF overrides the ON and the system will “Fail Silent”.

Computer Power Command Notional Block Diagram



Commands	State
NONE	OFF
BOTH	OFF
OFF	OFF
ON	ON

- Similarly, the “Over Current Sense” circuit designed to “fail Silent” by removing power to the circuitry and thus minimize the risk/threat of additional damage in the event of a continuously powered short circuit
  - Note that the “low side” current sensing would not detect shorts to chassis in a typical power reference to chassis configuration.

Fail Silent System Architecture

- A Fail Silent subsystem is a valid approach and has several advantages:
  - **Decreases the threat of a Byzantine fault (the computer unknowingly providing an incorrect answer)**
  - **Mitigates the separate risk/treat of collateral damage to the power system from continuous short**
  - **Provides a predictable system response with multiple redundant systems**
- A Fail Silent system architecture requires a multi-tiered configuration where the “last line of defense” is a “never give up” or “Safe-hold” system to take over when all computers go silent.
- A typical NASA robotic satellite utilizes a “Safe-hold” mode where a dissimilar, simple attitude control system is used to keep the spacecraft attitude stable and power positive in the event of an emergency.
- The presents of the Orbiter docked to ISS at this critical time and provided the dissimilar attitude control.

“Risk Based” Approach

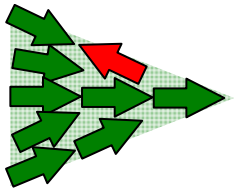
- The NESC’s Design Development Test and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems (Volume-II) focuses on creating a system that mitigates specific threats or risks to a given implementation

1 Eliminate the threat/risk from the design

[Reduce the threat/risk to equal probability/impact of other system threats/risks]

2 Reduce the Likelihood by decoupling system interactions

[Predictability: subsystem’s fault response consistent with system architecture]



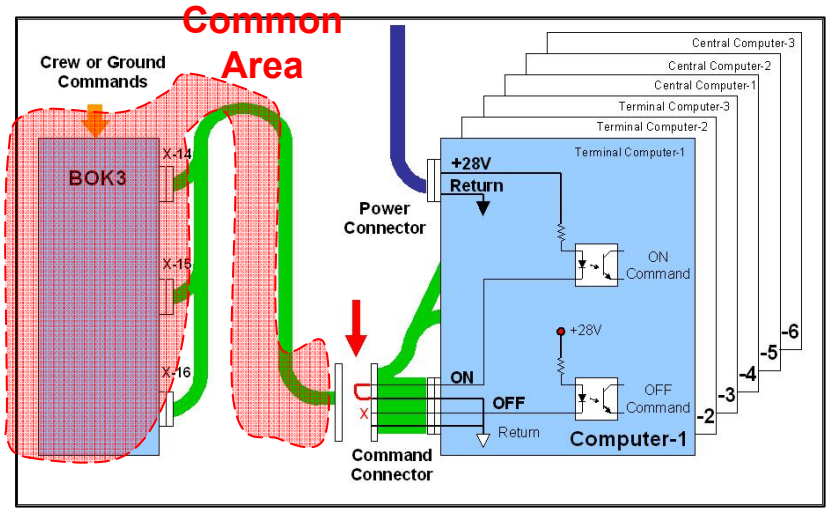
3 Mitigate the consequences by adding diverse redundancy

[Diverse redundant systems not simultaneously susceptible to threat/risk]

“Redundancy” Vulnerability

- The 12 computer commands (6-ON & 6-OFF) are common inside the BOK3, the three identical BOK3 connectors (X-14, X-15 & X-16) and associated harness.

- This common area creates a single point failure vulnerability where one single threat/risk can disrupt all six computers simultaneously



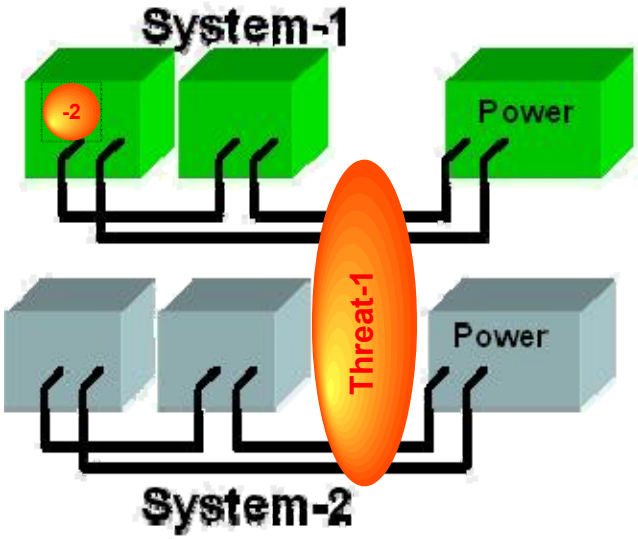
- A Failure Modes and Effects and Criticality Circuit Analysis (FMECA) is designed to capture these types of system’s single point failure vulnerabilities.

- The focus of a FMECA is to minimize the impact on the system of a single failure by physically separating redundant systems beyond the sphere of influence of that single failure.

Redundant Systems' Degree of Separation

- The required degree of separation is a function the "sphere of influence" of a probable threat/risk in physical relationship to the system implementation.

- In this example, redundancy is effective in mitigating Threat-2 (e.g., Part failure) but not effective at mitigating Threat-1 (e.g., condensation)



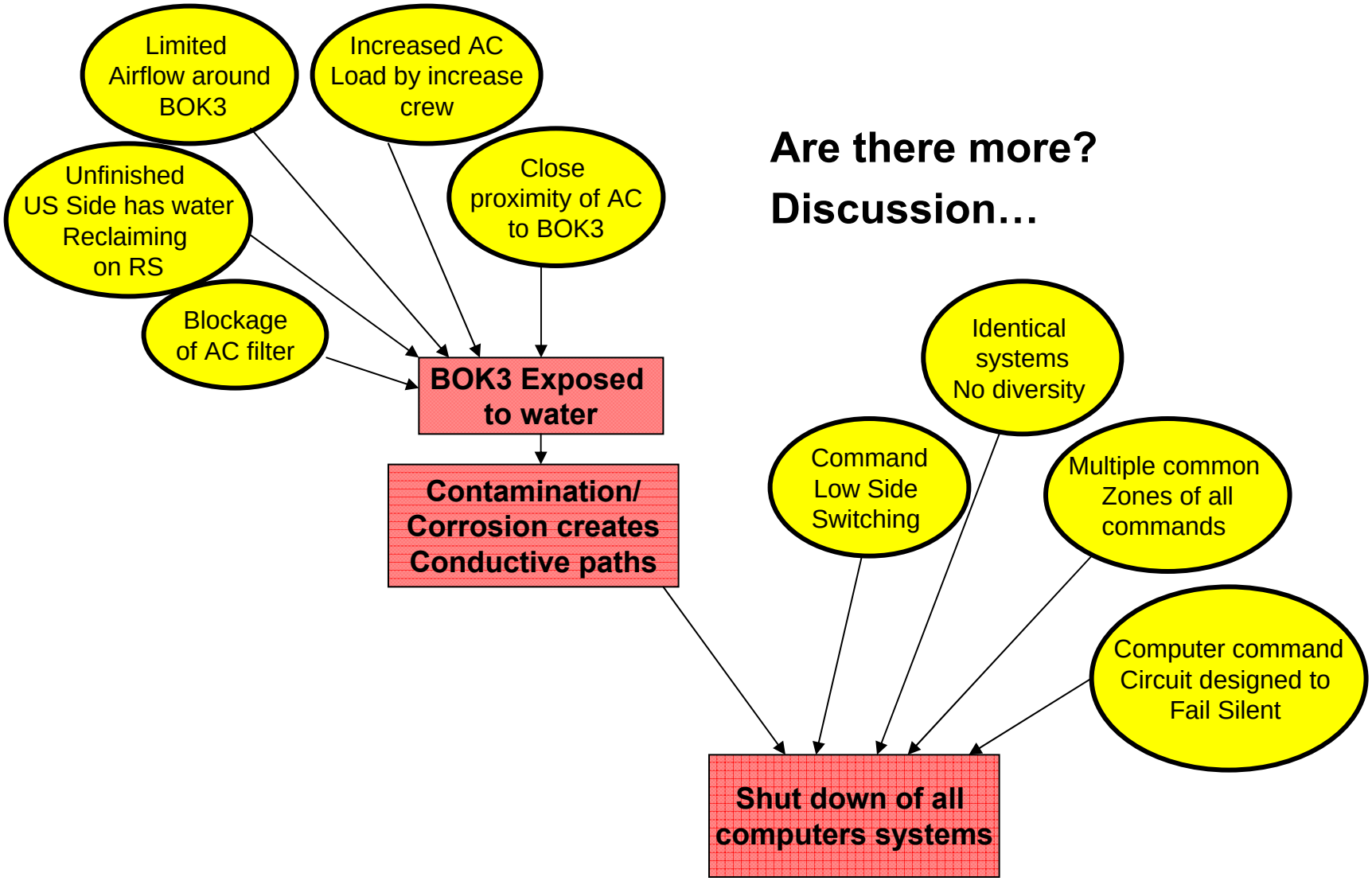
- There is no single design answer, rather a reliable and safe system is created by a process that mitigates probable threats by considering the sphere of influence of that threat relative to physical relationship to the system implementation.

- **If the threat/risk sphere of influence impacts more than one system the threat classification changes to "common cause".**

Conclusion

- Regardless of requirements, constraints and operational considerations momentary undesirable environments or interactions will occur eventually.
- How each and every individual subsystem responds to probable threats must be aligned in a system architecture to achieve a predictable and robust system.
- A reliable and safe system is created by *a process* that mitigates probable threats by considering the sphere of influence of each threat relative to the specific design implementation.
- A “common cause” threat/risk can be any threat/risk that impacts more than one system in a given implementation.
- For redundancy system architectures, the threat/risk mitigation effectiveness is a function of physical separation and/or dissimilar design implementation.
  - A dissimilar design has the advantage of reduced functionally to focus on safely and reliability. [less functions = less complexity = more predictability]
- Fail Silent system architecture requires a multi-tiered configuration where the “last line of defense” is a “never give up” or “Safe-hold” system to provide critical functions when all computers go silent.

Events of Interest



Are there more?

Discussion…