

Common Cause Failure Modes

Jon Wetherholt, NASA Marshall Space Flight Center, Huntsville, Alabama, USA
Timothy J. Heimann, NASA Marshall Space Flight Center, Huntsville, Alabama, USA

Keywords: common cause, redundancy

Abstract

High technology industries with high failure costs commonly use redundancy as a means to reduce risk. Redundant systems, whether similar or dissimilar, are susceptible to Common Cause Failures (CCF). CCF is not always considered in the design effort and, therefore, can be a major threat to success. There are several aspects to CCF which must be understood to perform an analysis which will find hidden issues that may negate redundancy. This paper will provide definition, types, a list of possible causes and some examples of CCF. Requirements and designs from NASA projects will be used in the paper as examples.

Introduction

Most projects/programs use failure tolerance as the primary and preferred approach to control hazards. Fault tolerance or graceful degradation is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. Redundancy is used most often to provide fault tolerance. But there are instances where all redundant systems fail due to a common cause failure mode. One simple definition of a common cause failure is “a failure of two or more components, system, or structures due to a single specific event or cause.” A more complex definition is “an event or cause which bypasses or invalidates redundancy or independence, i.e., an event which causes the simultaneous loss of redundant or independent items which may or may not include inadvertent operation, or an unintended cascading effect from other operations or failure within the system.” This definition includes the concept of operations. A major part of operations is the human element, which has been shown to be a contributor to common cause failures.

There is some thought that CCF is not typical and does not happen often. Airplane avionics is an example of data from a RGW Cherry & associates paper (Ref 1) which shows that an independent three-leg system has a much worse failure rate than three times the failure rate of one leg. The paper provides similar data for aircraft hydraulic systems. In this paper we will discuss some of the types and causes of CCF as well as providing some examples, both real and theoretical. We will also discuss techniques for reducing CCF.

Background

There are several contributing factors or causes for a common cause failure. The following is a brief list of causes which can take out redundant components or systems. Some of the items are inter-related.

- System or component requirements (may ignore several CCF factors)
- Wear out (If all similar items are old, they may be reaching the end of life together)
- Contamination (foreign object, chemical degradation, internal generated debris, etc.)
- Corrosion (inter-granular, corrosion fatigue, stress corrosion cracking)
- Environment
 - Weather (ice, rain, winds)
 - Lightning/Electromagnetic interference
 - Earthquake
 - Thermal conditions
- Loss of power
- Software (the hardware may be redundant but the software is the same version on all units)
- Saturation of signals (under sizing the data handling system)
- Design deficiency
- Lack of process control/manufacturing deficiency (all the items in the lot used are defective)
- Transportation/ shipping

Human error/system complexity (e.g. maintenance or installation errors)
Cascading (multi-channel systems with load sharing)
Single physical point where redundant items meet (examples: Hydraulic systems (common reservoir or common path for lines), Structures, Fire)

Examples

The first example is a theoretical example demonstrating several common cause failure initiators. This example is a RAID (Redundant Arrays of Inexpensive Disks) which is used to redundantly store information. When two disks are purchased online and are installed in a computer there can be many common modes of failure. The disks are likely from the same manufacturer and of the same model; therefore, they share the same design flaws. The disks are likely to have similar serial numbers, thus they may share any manufacturing flaws affecting production of the same batch. The disks are likely to have been shipped at the same time, thus they are likely to have suffered from the same transportation damage. As installed, both disks are attached to the same power supply, making them vulnerable to the same power supply issues. As installed, both disks are in the same case, making them vulnerable to the same overheating events. They will be both attached to the same card or motherboard, and driven by the same software, which may have the same bugs or viruses. Because of the very nature of RAID, both disks will be subjected to the same workload and to very (repetitive) similar access patterns, stressing them in the same way. They will also be the same age, hence late in life they may both fail at similar times.

An actual example demonstrating single physical point failure is the case of United Airlines Flight 232 which was flying from Denver, Colorado to Chicago-O'Hare. On July 19, 1989 on the DC-10, the number 2 engine (on the tail of the plane) experienced a failure which threw shrapnel into the hydraulic lines passing through a 10 inch wide channel in the tail. All three redundant hydraulic systems lost fluid, leading to loss of flight control surface actuation. The pilot used the thrust levers from the two remaining engines (one on each wing) to vary the thrust. In this way, increasing thrust would increase the pitch of the plane, creating a differential thrust between the two engines which would yaw/roll the plane. This technique was not ideal because it was not exact, and it was not essentially a fast response. This control difficulty can be gleaned from the air-to-ground recording in which the pilot (Alfred C. Haynes) demonstrates he kept his sense of humor which is vital in these situations:

Sioux City Approach: United Two Thirty-Two Heavy, the wind's currently three six zero at one one; three sixty at eleven. You're cleared to land on any runway.

Haynes: [laughter] Roger. [laughter] You want to be particular and make it a runway, huh?

The lack of fine control was evident in the approach to the runway. After dumping the fuel the crew was not able to line up on the runway assigned by the tower at Sioux City. The plane broke up on the runway during the emergency landing, killing 110 of the 258 passengers and one member of the eleven member crew. The pilot managed to use thrust modulation to control the aircraft, but this was not a designed-in redundancy for the system. This redundancy while not common to the other flight control method, which used hydraulics, could have been rendered inoperable if there was a common system between the two.

An example from the space program for a single physical point is the highly publicized Apollo 13 explosion. Bare wires in the number two oxygen tank located in the service module caused an arc when power flowed through them, igniting the liquid oxygen in the tank. Oxygen tank 1 and its redundant supply, oxygen tank 2, were located directly adjacent to each other. The concussion from the blast also damaged oxygen tank 1, causing it to leak, emptying its entire supply to space. This left the crew with no breathable oxygen in the command module, and no oxygen to power the fuel cells. The crew had to rely on the consumables in the lunar module, stretching them to their limit, to make the return trip to earth. One of the design corrections made to the lunar module after the failure investigation was to separate the oxygen tanks, placing them in separate equipment bays, such that a similar failure would have less chance of damaging both oxygen tanks. The lunar module providing redundancy for a situation such as this was not considered originally, but the different design and distance from the service module proved to eliminate several CCF modes.

An example of a cascading failure is the east coast black out of 2003 (ref 3). In the east coast grid there are several sources of generating power, and the lines that carry the power are redundant. But during the summer when the loads are high the system is stressed. The lines that transmit the power heat up as the through current increases. This causes the lines to sag. After one line fails and the current is routed through parallel lines, (not always co-located) those lines heat up and sag more. This sag may bring the parallel line into contact with trees or other objects causing a short. The breaker tripping increases the load on the other parallel lines. More sag ensues. See figure 1 from the report. This is the scenario believed to have been a contributor to this failure which shut down over 100 generating plants, affecting a total of approximately 55 million people.

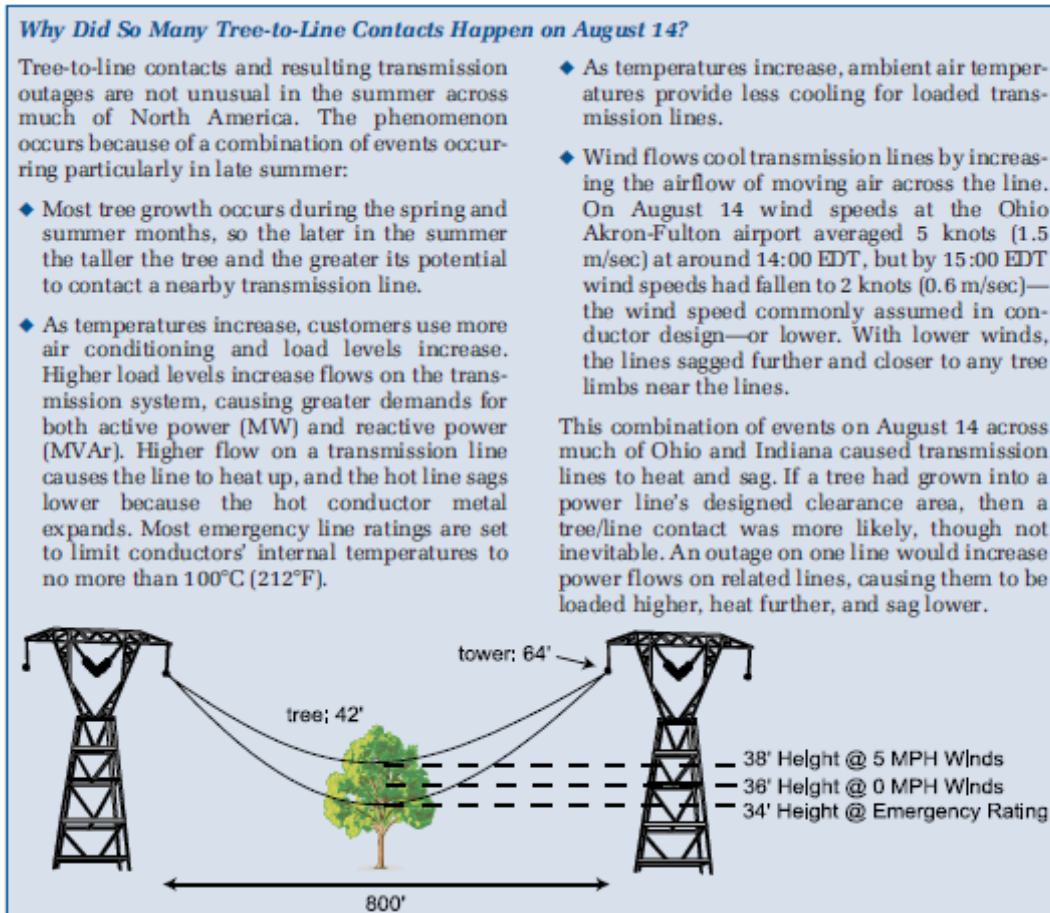


Figure 1. U.S.-Canada Power System Outage Task Force August 14th Blackout: Causes and Recommendations

An example of human error in the airline industry occurred when a DC-10 cabin door blew out on Flight 96 from Detroit to New York. (Ref 4) The DC-10 had an outward swinging cargo door. An inward swinging door takes up more cargo space, but when the plane is under pressure it is held shut. If an outward swinging door is not latched, inside pressure can blow the door out. The outward door required the baggage handler to perform three tasks to safely lock the door. He had to pull down a top-hinging door to shut it, then swing down a lever on the outside of the door, and then press and hold a button that operated an electric motor at the top of the door. With his ear to the fuselage, he was supposed to hold the button until he heard a click and wait for seven seconds until he heard the motor stop. If the motor did not finish lowering the latches, the door would appear to be closed until the airplane reached an altitude where the pressure was great enough to blow out the door. The failure modes and effects analysis had indicated this. In a cabin pressure test of its first airplane this scenario happened. The fix was a hole in the door for a vent flap that would close when the linkage that shut the door was engaged. If there was leakage the pilots would know there was a problem before the door blew open and they could return to the airport. An

additional problem was that the handler could make the vent flap close by excessive force even without the door locked. This is what occurred in Detroit on June 12, 1972. The doors were notoriously hard to close, so the handler was not surprised by the difficulty in closing. He had put his knee on the closing lever and the door shut, but the vent flap did not appear correct. He called a mechanic who opened and shut the door. The warning light in the cockpit went out only because the handler's weight on the door had bent the metal linkage in the door. The door was not completely locked but the vent flap was closed. When the plane reached twelve thousand feet, the door blew open and part of the floor collapsed, blocking the cables to the tail. This jammed the rudder. Fortunately the pilot had trained to steer the plane using the two wing engines, and did so successfully, bringing the plane to a safe landing. When designing systems for everyday use with human interface, CCF must be closely explored.

Finally a recent example of an environmental CCF is Japan's Fukushima Daiichi Power Plant. In this case the backup generators used to generate power if an earthquake interrupted power failed due to the water from a tsunami flooding the system. The thought of the CCF of an earthquake both causing power loss and a tsunami of sufficient size to overcome the wall created to protect the plant was not envisioned.

Reducing CCF

Using the list in the background section, a check list of items to look for can be created which will allow the engineer to search for CCF modes and eliminate them or reduce their likelihood. The following examples with mitigations explore this.

Contamination can be a source of common cause failure. In the case of a space system where air flow is required for life support, redundant means of performing the function may be required. Contamination can be controlled by a number of means; the simplest is a filter immediately upstream of the first fan covers to stop unforeseen contamination in the system, see figure 2.

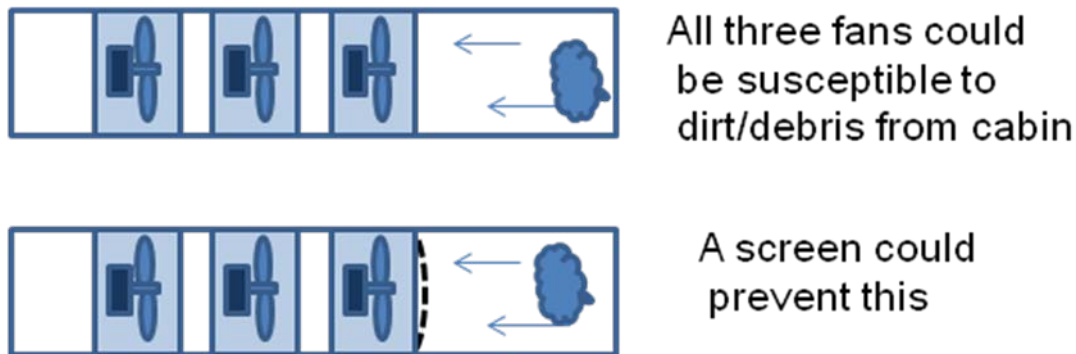


Figure 2

This does not protect the other two fans if there is contamination created by the first fan in the series, which could be a cascading failure. See figure 3.



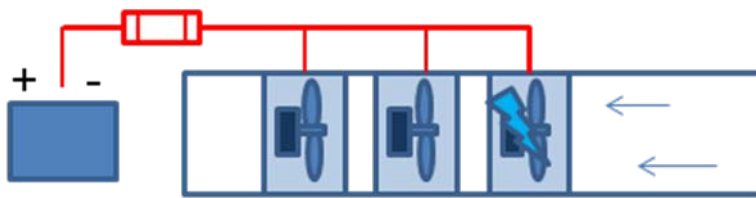
One fan can fail, sending debris into other fans, a cascading failure



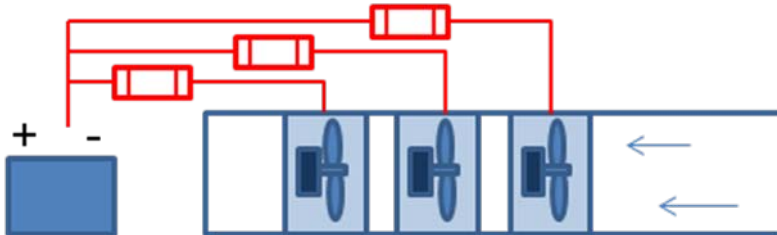
Each fan having a screen will limit this

Figure 3

Common protection schemes for failures which cause hazards may insure a hazard does not occur, but the scheme may eliminate the function. In the case of a space system where air flow is a life support requirement this would create a hazard in itself. See figure 4.



All three fans could be susceptible to loss of power if one fan has a short



Each fan having a fuse will limit this

Figure 4

The power source could also fail which would lead to the loss of function and therefore a loss of life. See figure 5.

Common Source Cause Failure

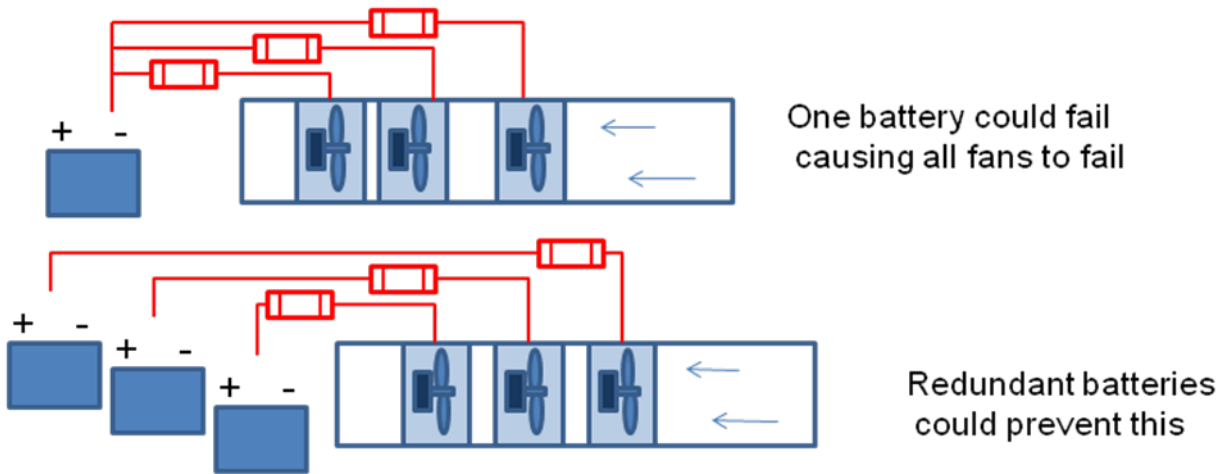


Figure 5

On a space experiment, unlike redundancy is used to reduce the likelihood of CCF. The purpose of the system is to fill a chamber for an experiment from a high pressure bottle. See figure 6. For science purposes, the primary pressure control is a pressure transducer on the chamber connected to a computer which, operating a solenoid valve. If this fails the regulator would keep the pressure below the chamber maximum pressure. If the regulator fails a pressure switch downstream will trip, closing the valve upstream of the regulator, preventing regulator failure-generated particles from failing the valve. A filter not shown in the diagram upstream of the valve prevents the valve from becoming contaminated by the bottle contents. Finally the chamber pressure switch shuts a valve if the chamber pressure is too high. The use of a regulator, a pressure transducer/computer/valve and a pressure switch combined with a valve covers many of the aspects of the above list. Some of the devices being totally mechanical prevent the Electromagnetic Interference CCFM from occurring. All the components are manufactured by different vendors. Test procedures for each item are different enough to reduce human error. Each system tripped at a different pressure so that once the system is assembled each control could be tested. This experiment is currently in operation on the space station.

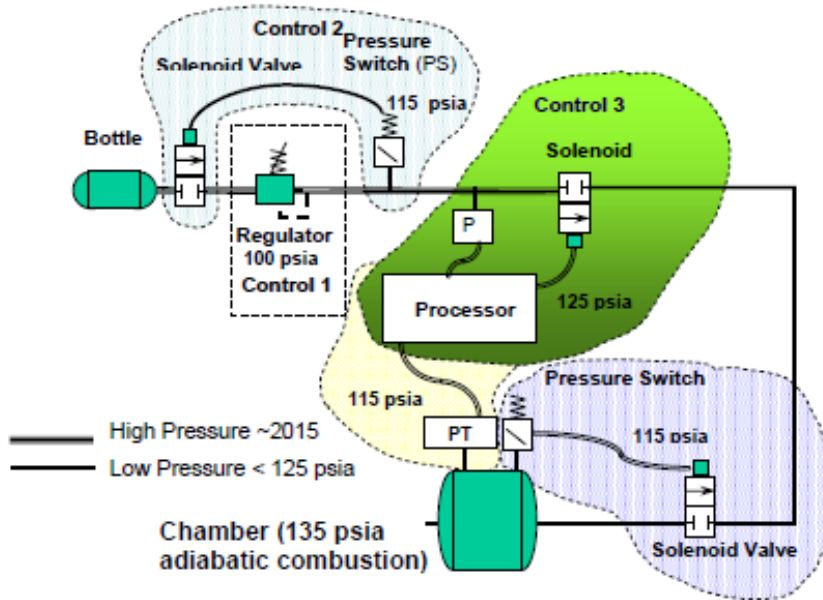


Figure 6

Software is a common failure point for most modern systems. The software is expected to handle more of the system load from safety critical functions to mundane data handling, and therefore can be very complex. This leads to being unable to foresee all combinations of conditions for the software. Therefore, not all conditions can be tested. Although the hardware may be redundant, the software running on both computers is exactly the same in most cases. Failures such as input data out of range, unbounded execution, arithmetic errors, and uninitialized variables or pointers will have the same affect on all computers. Single point software must have internal checks to seek problems. This can be done, for example, by the software range checking input data and including watch dog timers.

Solutions

One of the most important considerations in reducing CCFM is knowing that they can exist and what the most common modes are. Using a check list from several sources of literature and using a fault tree can help find the CCF modes. A step by step process starts with defining and understanding the system which includes modeling. One analytical/modeling technique is to use a fault tree to formally identify failure modes and their interactions. There are several sources for performing fault tree analysis, the book “Hazard Analysis Techniques for System Safety” (Ref 5) II is an excellent source. Other models can be useful such as those which show the inputs to the system such as power or cooling, show the surrounding environment for the system such as weather or factory floor, or show engineering design such as circuit or fluids diagrams. Reference 5 also has a chapter on a detailed approach to CCF analysis.

Conclusion

Common Cause Failure modes are prevalent and must be addressed by the safety community. There are several levels that CCF can act upon, and choosing a control at the proper level can provide wide protection. While unlike redundancy is a good start, there are CCF modes which can circumvent unlike redundancy which is why a thorough analysis is necessary. Expressing the concern with the engineering team and discussing simple methods to reduce or eliminate CCF will aid in producing achievable results.

References

1. SYSTEM SAFETY ASSESSMENT COURSE, R.G.W. Cherry & Associates Limited 2008. Available at <http://www.rgwcherry.co.uk/download/Common%20Cause%20Failures.pdf> . Accessed April 4, 2011.
2. United Airlines Flight 232. Available at http://en.wikipedia.org/wiki/United_Airlines_Flight_232. Accessed April 4, 2011.
3. U.S.-Canada Power System Outage Task Force Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations April 2004. Available at <https://reports.energy.gov/> . Accessed April 4, 2011.
4. Inviting Disaster James R. Chiles, Harper Business, 2001, 2002.
5. Hazard Analysis Techniques for System Safety, Wiley 2005, Clifton A. Ericson II

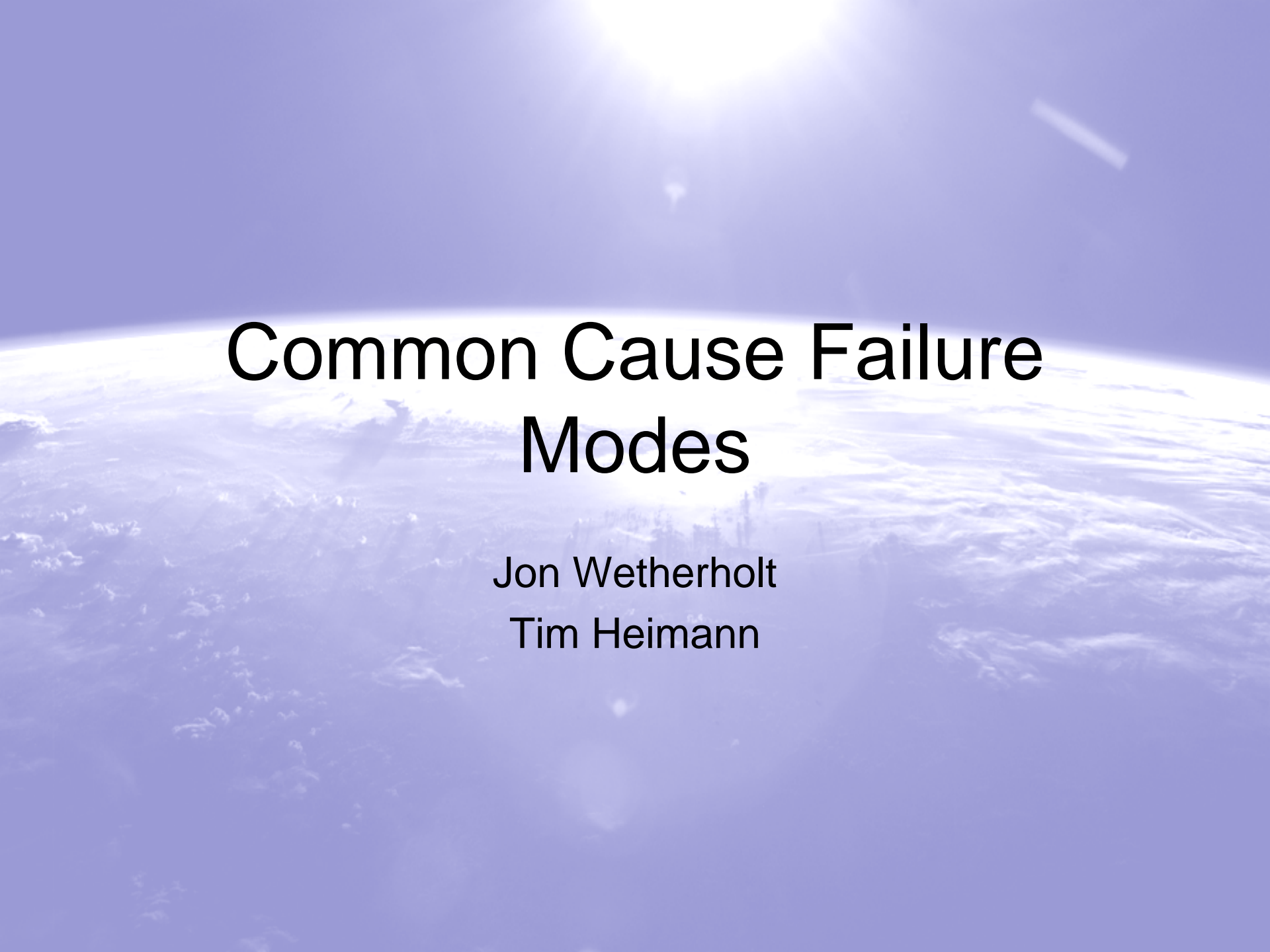
Biography

Jon Wetherholt, NASA Marshall Space Flight Center, Huntsville, Alabama, 35812, USA Telephone (256) 544-4847, email – jon.c.wetherholt@nasa.gov

Mr. Wetherholt has more than 27 years of experience in system safety and product assurance. Mr. Wetherholt currently is the lead for Ares Vehicle Integration System Safety at the Marshall Space Flight Center in Huntsville, Alabama.

Timothy J. Heimann, NASA Marshall Space Flight Center, Huntsville, Alabama, 35812, USA Telephone (256) 544- 3016, email - timothy.j.heimann@nasa.gov

Mr. Heimann maintains more than 26 years experience in the field of Systems Safety Engineering; the last 20 dedicated to Space Systems Safety. Since April 2008, he has been working with Bastion Technologies Incorporated at the Marshal Space Flight Center as a System Safety Engineering Lead and as Executive Officer for the Constellation Safety and Engineering Review Panel (CSERP).



Common Cause Failure Modes

Jon Wetherholt
Tim Heimann

Introduction

- High technology industries with high failure costs commonly use redundancy as a means to reduce risk
- Redundant systems, whether similar or dissimilar, are susceptible to Common Cause Failures (CCF)
- There are several aspects to CCF which must be understood to perform an analysis which will find hidden issues that may negate redundancy

Types of CCFM

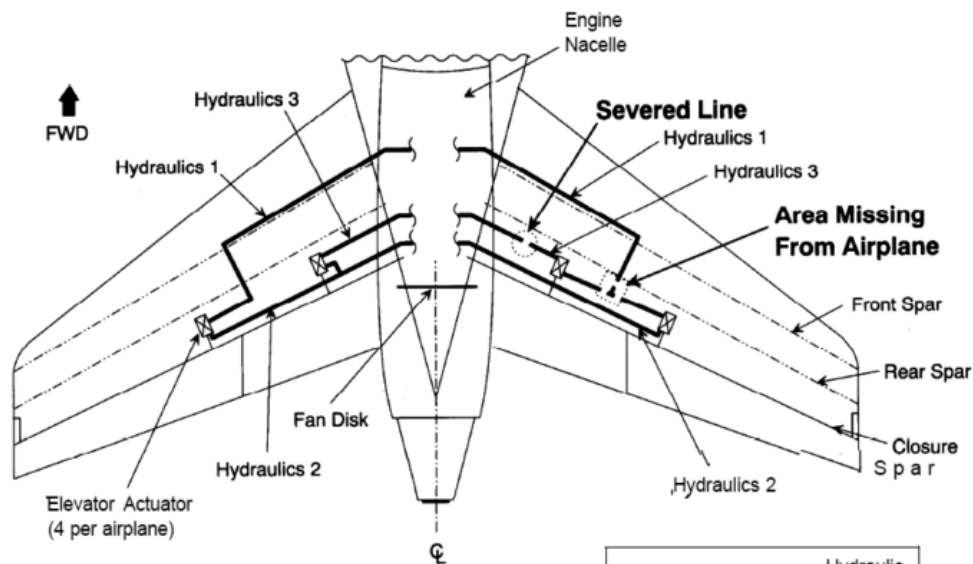
- System or component requirements (may ignore several CCF factors)
- Wear out (If similar items are old, they may reach the end of life together)
- Contamination (foreign object, chemical degradation, internal debris, etc.)
- Corrosion (inter-granular, corrosion fatigue, stress corrosion cracking)
- Environment, Weather (ice, rain, winds), Lightning/Electromagnetic interference, Earthquake, or Thermal conditions
- Loss of power
- Software (the hardware may be redundant but the software is the same version on all units)
- Saturation of signals (under sizing the data handling system)
- Design deficiency
- Lack of process control/manufacturing deficiency (defective lot used for items)
- Transportation/ shipping
- Human error/system complexity (e.g. maintenance or installation errors)
- Cascading (multi-channel systems with load sharing)
- Single physical point where redundant items meet (examples: Hydraulic systems (common reservoir or common path for lines), Structures, Fire)



DC-10 Hydraulics

(Single Physical Point)

All 3 redundant hydraulic systems were cut by single engine failure



Not to Scale

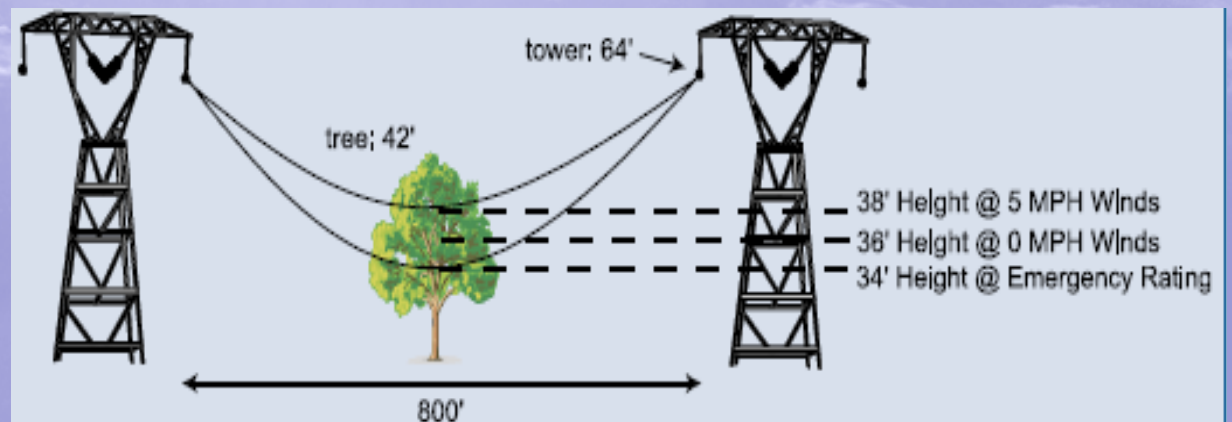
Actuator Position	Hydraulic System
RH Inbd Elev	1 & 3
LH Inbd Elev	2 & 3
RH Outbd Elev	1 & 2
LH Outbd Elev	1 & 2

Non-designed in redundancy, using remaining two engines to control the plane, saved many lives

Power Grid

(Cascading Failure)

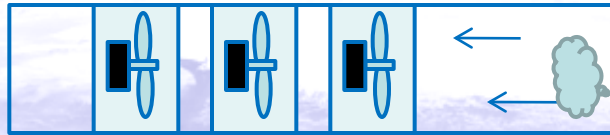
- Hot day
 - Led to increased power consumption
 - Led to power lines sagging
- One set of power lines were lost increasing load on remaining lines
 - Those lines sagged



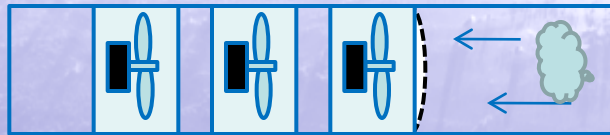
Environmental Control Fan

(Debris Causing Cascading Failure)

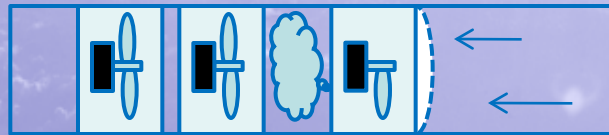
On orbit, air flow is required to maintain life



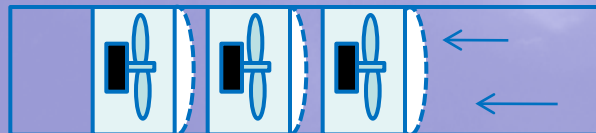
All three fans could be susceptible to dirt/debris from cabin



A screen could prevent this



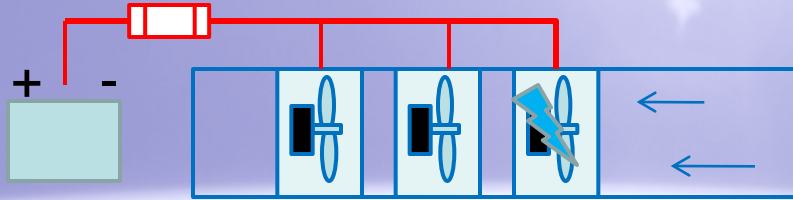
One fan can fail, sending debris into other fans, a cascading failure



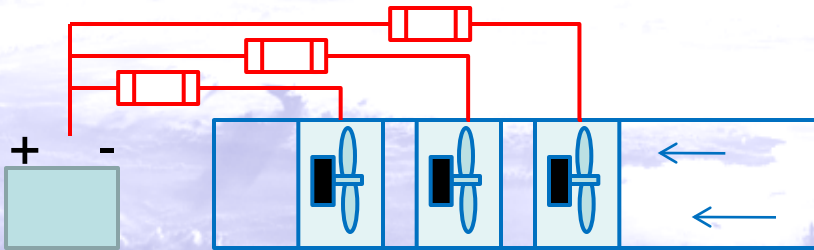
Each fan having a screen will limit this

Environmental Control Fan

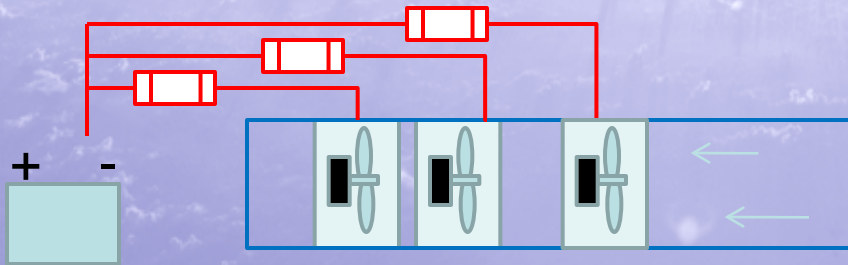
(Requirements & Power Failure)



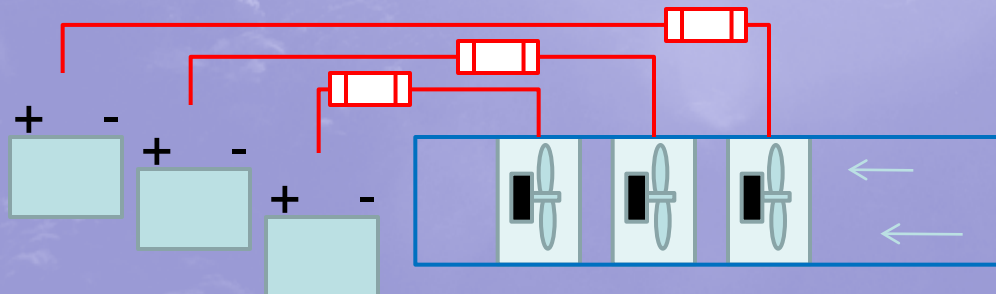
All three fans could be susceptible to loss of power if one fan has a short



Each fan having a fuse will limit this



One battery could fail causing all fans to fail



Redundant batteries could prevent this

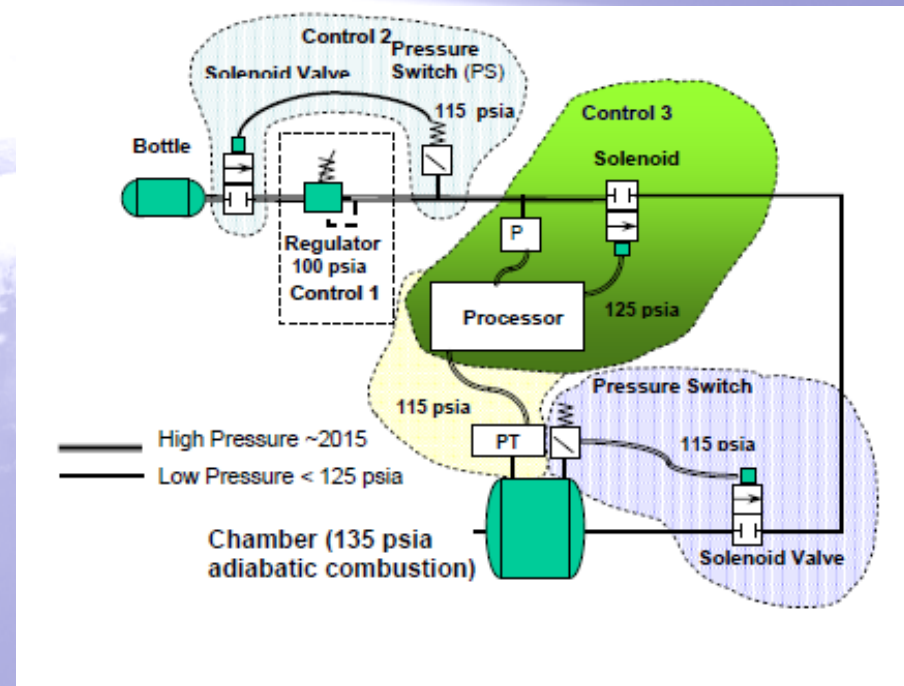
Avionics & Software

- Avionics and Software is probably the most difficult to assess and prevent
 - Unlike redundant avionics are expensive
 - May have common electronic components as well
 - Unlike software is expensive
 - Will have common requirements set
 - Understanding all the contributing inputs to software is near impossible
 - Understanding all the interactions in software is improbable
- If possible back up safety critical avionics function with hardware only

Pressure fill system

(Unlike Redundancy)

- PT/Processor/Solenoid Susceptible to:
 - Power failure (if fail open)
 - Contamination
- Regulator Susceptible to
 - Corrosion
 - Contamination
 - Wear out
- Solenoid/PS Susceptible to
 - Corrosion
 - Contamination
 - Power failure (if fail open)



Recommendations

- Perform a Fault Tree Analysis
 - Defines interactions and common failure paths
 - Can be done on system level and can be performed on subsystems or components that contain redundant items which are deemed susceptible
- Use a common cause failure list
- Use un-like redundancy when possible

Summary

- Common Cause Failure modes are prevalent and must be addressed by the safety community.
- There are several levels that CCF can act upon, and choosing a control at the proper level can provide wide protection.
- While unlike redundancy is a good start, there are CCF modes which can circumvent unlike redundancy which is why a thorough analysis is necessary.