Developing Electronic Systems for Safety-Critical Applications

Rob Hammett
Draper
Cambridge, MA
617-258-2494
rhammett@draper.com
Tutorial Outline

• Introduction
• System Safety Basics
• Techniques to Make Electronics Safe (with examples)
• Design of Fault-tolerant Systems
• Conclusion
Otis Elevator Safety Brake Enabled Skyscraper Construction
Modern trains rely upon a fail-safe air brake system that is based upon a design patented by George Westinghouse on March 5, 1868. The Westinghouse Air Brake Company (WABCO) was subsequently organized to manufacture and sell Westinghouse's invention. In various forms, it has been nearly universally adopted.

The Westinghouse system uses air pressure to charge air reservoirs (tanks) on each car. Full air pressure signals each car to release the brakes. A reduction or loss of air pressure signals each car to apply its brakes, using the compressed air in its reservoirs.[2]
Electronics Providing Critical Functions

- Safety-critical electronics are everywhere!
- A system is safety critical if …
  - System malfunction could cause harm
  - Loss of function could cause harm
  - Provides information that if incorrect could cause harm
- The design of these electronics must consider
  - Impact of hardware and software failures
  - Human limitations
  - Design deficiencies
Electronics / Computers – Very Capable, but Trustworthy?

Advantages

• Able to control systems a human can’t (e.g. unstable aircraft)
• Able to operate without human intervention (drones, self-driving cars, 24/7 monitoring)
• Very precise and efficient control
• Lighter weight, easier to maintain, more reliable, less costly than mechanical controls
• Can improve safety
  – Detect and mitigate hazards, including human error
  – Can be made fault-tolerant

Drawbacks

• Electronics don’t fail gracefully
• Increased complexity
  – Is it still working correctly?
  – Potential design errors

Great care is required to design electronics to operate safely
Electronic Failures Root Causes

- Defects in electrical interconnections
  - Wiring, connectors, solder joints, shorted signals...
  - Interruptions, transients in electric power sources
- Environmental
  - EMI, over temperature, corrosion, radiation ..
- Defects in piece parts
  - Manufactured in
  - Aging
  - Overstress
- Design errors
  - Hardware
  - Software
  - Not addressing sensor limitations
- Cyber attack

Safety-critical systems must be designed to address all failure causes
Electronic Failures – Software Errors

- Software does not fail, its design deficiencies are revealed
- Real-time software is difficult
- Interactions between hardware and software are complex, difficult to analyze
  - Interrupts are evil!
  - Combination of programmable hardware and software very powerful, and very complex
- Software changes are likely and may have unexpected consequences
- Specifying desired software behavior, particularly for off-nominal cases, is challenging
- Not practical to test all possible combinations of operating conditions, failures, time of failure, failure modes

These difficulties often lead to the use of alternative safety modes that don’t use software or use dissimilar software
Electronic Failures May be Transient or Permanent

• Transient
  – Fault condition is brief, hardware is not damaged
  – Fault condition is self-clearing, is cleared by cycling power or by another reset action
  – One cause of transient faults are space “cosmic ray” single event upsets (memory bit flips)

• Intermittent
  – Fault condition comes and goes
  – Requires a repair

• Permanent
  – Fault condition is constant
  – Requires a repair
## Examples of Electronic Control Mishaps

<table>
<thead>
<tr>
<th>Accident</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer controlled X-ray machine delivered fatal overdoses</td>
<td>Keyboard entry software – operator could enter keystrokes faster than system could correctly process them</td>
</tr>
<tr>
<td>Arien 5 launch vehicle explodes on launch</td>
<td>Unhandled software exceptions cause both primary and back controls to disengage</td>
</tr>
<tr>
<td>Tesla automobile crash using its “autopilot” feature</td>
<td>Computer vision algorithm failed to detect left turning truck, driver failed to take action</td>
</tr>
</tbody>
</table>

However…Many examples where electronic controls prevented accidents
Fault-tolerant Space Shuttle Electronics Prevented Accident

Redundant, fault-tolerant avionics prevented the loss of the space shuttle and its Chandra telescope payload.

July 23, 1999 – 5 seconds after launch an electrical short knocks out power to one side of 2 of 3 redundant main engine controls.
Apollo Missions Encountered Electronic Safety Issues

Apollo 11 Lunar Landing experienced software overrun alarms during first lunar landing

Steely-eyed missile man Neil Armstrong ignored them and landed safely

Apollo 14 Lunar Lander experience false “abort” switch signals prior to landing attempt due to floating solder ball

A software patch was quickly devised as a work-around to allow the landing
System Safety Basics
Simplified System Safety Process

1. Identify system hazards
2. Evaluate the mishap risk from these hazards
3. Classify / quantify hazards by risk level
4. Develop appropriate risk mitigations
5. Evaluate risk improvement
6. Gain approval that reduced risk is acceptable

These steps are repeated during:
- Concept development
- Design
- Deployment

Focus of this tutorial is on designing electronics to mitigate risks

Hazards – a condition that could cause death, damage, etc
Mishap – unplanned event that results death, damage, etc

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494
Safety is Risk Management - Risk Depends Upon Likelyhood and Consequences

Table 4.6  Risk classifications from draft IEC 1508. (IEC 61508)

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Catastrophic</th>
<th>Critical</th>
<th>Marginal</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>II</td>
</tr>
<tr>
<td>Probable</td>
<td>I</td>
<td>II</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>Occasional</td>
<td>I</td>
<td>II</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>Remote</td>
<td>II</td>
<td>III</td>
<td>III</td>
<td>IV</td>
</tr>
<tr>
<td>Improbable</td>
<td>III</td>
<td>III</td>
<td>IV</td>
<td>IV</td>
</tr>
<tr>
<td>Incredible</td>
<td>IV</td>
<td>IV</td>
<td>IV</td>
<td>IV</td>
</tr>
</tbody>
</table>

High risk

Low risk

Table 4.7  Interpretation of risk classes from draft IEC 1508.

<table>
<thead>
<tr>
<th>Risk class</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Intolerable risk</td>
</tr>
<tr>
<td>II</td>
<td>Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained</td>
</tr>
<tr>
<td>III</td>
<td>Tolerable risk if the cost of risk reduction would exceed the improvement gained</td>
</tr>
<tr>
<td>IV</td>
<td>Negligible risk</td>
</tr>
</tbody>
</table>
Design of safe systems begins with identification of hazards and the functional failures leading to hazards

Automobile cruise control example

(faulty speed sensor indicates low speed) (opens throttle to increase speed) (unintended acceleration) (can result in collision)
Quantifying the Frequency (Probability) of Failures

- Frequency of failure (per operating hour):
  - Frequent: $10^{-0}$
  - Reasonably probable: $10^{-1}$, $10^{-2}$
  - Remote: $10^{-3}$, $10^{-4}$, $10^{-5}$
  - Extremely remote: $10^{-6}$, $10^{-7}$, $10^{-8}$, $10^{-9}$


(FAA requirement for commercial aircraft) (.99999 - Apollo)
Examples of Frequency (Probability) of Failures

<table>
<thead>
<tr>
<th>Probability</th>
<th>Frequency</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely Improbable</td>
<td>Extremely Remote</td>
<td>Requires redundancy and fault-tolerant design</td>
</tr>
<tr>
<td>Improbable</td>
<td>Remote</td>
<td>High quality electronics – failure can be sudden with unpredictable performance, no benefit from preventative maintenance</td>
</tr>
<tr>
<td>Probable</td>
<td>Reasonably probable</td>
<td>Typical Mechanical parts – failure is generally gradual with predictable degradation in performance, preventative maintenance helps</td>
</tr>
<tr>
<td></td>
<td>Frequent</td>
<td>SOURCE “SAFETY CRITICAL COMPUTER SYSTEMS” BY NEIL STORY, ADDISON-WESLEY</td>
</tr>
</tbody>
</table>
Examples of Consequences of Failures

- **Catastrophic**
  - Loss of life, extreme environmental impact
  - Examples: Plane crash, Large Explosion

- **Critical**
  - Severe Injury, major environmental impact
  - Examples: Chemical exposure, Oil spill

- **Marginal**
  - Injury, major property damage
  - Examples: Machinery accident, Non fatal car crash

- **Negligible**
  - Inconvenience, minor damage
  - Examples: Interruption in service
System Complexity

Simple Fail-safe
  Loss of function not hazardous

Fail degraded
  Partial loss of function not hazardous

Fail Operational (Fail op)
  Simple functions
    Simple PID controller
  Complex functions
    Complex software flight control algorithms
  Time criticality of interruptions
    Ship’s rudder – loss of control for seconds to engage back-up OK
    Rocket – Must engage back-up within milliseconds to avoid loss of control

Disengage auto pilot, human assumes control
Switch from fully automatic to partial automatic
Techniques to Make Electronics Safe

- Fault avoidance (design for high reliability, e.g. low probability)
- Self-test and status reporting
- Passive failure modes
- Human monitoring and intervention (HMI)
- Safety mechanisms
- Back-up systems
- Fault-tolerant systems
- Hybrids – Combinations of monitoring, safety mechanisms, back-ups and human intervention
Fault Avoidance

- **Quality control**
  - Qualification
  - Inspection
  - Burn-in
  - Accelerated life testing

- **Disciplined development process**
  - Requirements and requirements verification
  - Design visibility and peer reviews
  - Extensive, realistic testing

- **Conservative design**
  - Derating
  - Benign failure modes
Self Test and Status Reporting

- Embedded computers and software facilitate self-test
- Different types
  - Power-on Self Test (POST)
  - Initiated self test (often intrusive)
  - Continuous self test
    - Fault Detection, Isolation, Reconfiguration (FDIR)
    - Mechanical / hydraulic performance monitoring
- Thoroughness (coverage) of self-test is a safety consideration
  - Undetected failures provide no warning to operator
  - If undetected, fail-safe modes or back-up systems not engaged
Passive Failure Modes

• Preliminary Hazard Analysis (PHA) can identify the system modes of failure with most severe consequences
• Electronics can be designed to be more likely to fail to less severe modes
• Example – Voltage for automobile “gas” pedal

Throttle pedal generates voltage proportional to desired speed

Design option #1
0 volts = max speed
10 volts = min speed

Design option #2
0 volts = min speed
10 volts = max speed

Fail to min speed – marginal consequence
Fail to max speed – serious consequence
Likelihood of 0 volt failure – high
Likelihood of 10 volt failure – low
Design option #2 increases system safety
Other Passive Failure Mode Design Examples

- Electronic valves that fail to safest condition if power is removed
  - Valve closed to stop flow of fuel, stop the engine
  - Valve to mid stroke position to provide “limp home” operation
- All computer outputs are safe when no electrical output is produced
  - Computer watchdog timer inhibits all outputs if computer “crashes”
- Displays are blank or provide a warning when not being refreshed
- Sensors designed to fail producing data that computer can easily recognized as invalid
Human Monitoring and Intervention (HMI)

• Human monitoring
  – Typically alerted by system alarms
  – Human senses (noise, smoke, vibration,…) or other instrumentation
  – Historical knowledge facilitates fault detection, isolation

• Human intervention
  – Cost effective back-up for infrequent events
  – Improvise for unplanned situations

• Human limitations
  – Limited reaction times
  – Limited attention span
  – 24/7 monitoring not practical
  – Not present in unmanned systems
HMI Example - Automotive Cruise Control

Potential safety hazards
- Disengagement causing loss of speed
- Undesired acceleration

Characteristic
- Interruptions in service acceptable
- No failure detection or alarm provided (human discovers loss of speed)
- Human override to disengage (on/off switch)
- Delayed repair acceptable for restoring service

Presence of an attentive human operator is required to avert hazards
Safety Mechanisms

- If system risks are too great, safety mechanisms can be a cost effective mitigation
- A typical safety mechanism is independent of the primary control system, senses a high risk hazard and mitigates it
- Examples include devices that sense overheating, overpressure, and excess speed and take positive action to make the system safe (remove power, shut off fuel,...)
- Other safety mechanism include safety switches and interlocks
  - Safety switches and interlocks are generally used to prevent a machine from harming its operator or damaging itself
  - Examples - Microwave oven won’t work with the door open, machine will not operate without a load applied to prevent destructive overspeed
Safety Mechanism Example – Gas Water Heater

Function
• Turn gas burner on/off to maintain hot water temperature

Consequences of loss of function
• No hot water, inconvenience

Consequences of malfunction
• Water tank explosion
• Gas explosion
• Loss of life and property

Probability of malfunction
• Pilot light extinguished by drafts
• Mass produced gas control valve subject to manufacturing or installation defects

Safety mechanisms
• Pilot light thermocouple cutoff of gas valve
• Simple P&T relief valve vents excess pressure
Gas Water Heater Failure

- T&P relief valve
- Gas control valve
- Thermocouple

Simple, inexpensive safety mechanisms make this dangerous system safe
Safety Achieved by Simple Back-up

Two Engine Aircraft

Two Smoke Detectors

Two Radios in Aircraft
Jet Engine FADEC – Back-up, Safety Mechanism, HMI

- Includes two electronic controls, primary and back-up
- Automatic switchover to back-up provides same functions as primary (fly until convenient to service)
- Mechanical over speed protection insures no hazard to aircraft, provides takeoff thrust
- Pilot can shut down one engine and land safely on remaining engine
Satellite Control – Automatic Monitoring to Achieve Safe State, HMI Switchover to Back-up

- Satellite in intermittent contact with human operator (partially autonomous)
- Autonomous health monitoring, go to safe state upon detected failure
- Operator can control in safe state, power-up and initialize a cold back-up

I am in safe mode!
Switch to back-up
Automotive Throttle-by-wire

Function
• Regulate engine speed based on drivers gas pedal, vehicle speed, temperature, transmission,…

Consequences of loss of function
• Sudden deceleration, inability to maintain safe speed

Consequences of malfunction
• Unexpected acceleration
• Inability to reduce speed

Probability of malfunction
• Includes software of significant complexity

Safety features
• Driver can apply brakes, place in neutral, turn off engine
• Dual redundant pedal and throttle valve position sensors for failure detection, safe mode activation
• Throttle valve spring returned to mid speed if servo motor not applying torque
• ECM fails to “no servo torque” for most elect failures
• Software subject to development and test rigor
Automotive Throttle-by-wire

Observations
- Loss of service creates safety risks (sudden deceleration at highway speeds) and significant inconvenience (towing)
- Auto-acceleration malfunction may exceed skills of driver to insure safety
- Safety depends upon presence of attentive driver
- Repair required to restore function with inconvenient interruption in service
- Software a significant safety concern
- Addition of redundant sensors, ECM design features, software development are added costs

Presence of an human driver is required to avert hazards

Despite well publicized issues, overall safety record is good and performance advantages are significant

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494
Automotive Steer-by-wire

Electric Power Steering (EPS)

- Automatic lane keeping
- Self parking
- Trailer backing assist

Criticism: Steering wheel force is very high following loss of function

Steer-by-wire (Infinity Q50)

- Allows variable ratio steering
- Supports all EPS features

Higher risk: System must engage clutch if elects fail

• Triple redundant ECU’s
• Torque sensor & force feedback
• Elect motors
• Clutch to disengage Mech link

Mech link
Torque sensor
Elect motor assist & ECU

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494
Aircraft Fly-by-Wire

- Note single engine!

- No manual control by pilot available or possible

Quad redundant voting fly-by-wire
Fly-by-wire Aircraft Overview

Function
• Modulate aircraft control surfaces (aileron, rudder) to maintain aircraft attitude, heading, altitude, speed

Consequences of loss of function
• Inability to maintain safe flight and landing

Consequences of malfunction
• Inability to maintain safe flight and landing

Probability of malfunction
• High quality equipment, well maintained
• Significant complexity can introduce design and maintenance errors

Safety features
• Makes use of redundancy and fault-tolerance for hardware defects
• Software process and dissimilar control features to mitigate design detects
• Ejection seat on military aircraft

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494

38
Safety-Critical “One Shot” Functions

- One shot functions are irreversible
- Typically, they “must work” at the correct time to prevent an unsafe condition
- Typically, they “must not work” at the wrong time to prevent an unsafe condition
- A challenging problem for the electronics designer

Auto airbags
Parachutes
Stage separation
Automotive Airbag Control

Simple, dissimilar interlock to prevent unwanted deployment (must not work)

Continuous self-test monitoring air bag readiness is critical to safety (must work)

Other safety considerations – EMI, installation and maintenance
Space Shuttle Solid Rocket Booster Separation

A simple, dissimilar interlock not possible – only complex software can correctly initiate
Self-Driving Cars Evolved from Vision-based Control of Mobile Robots

- Deceptively complex problem
- Involves image recognition & Simultaneous Localization and Mapping (SLAM) algorithm
- Safety risks arise when human are involved, speeds and mass increase and the environment becomes much more complex

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494
Self-Driving Cars in the Real World

Safety Issues

• Hardware must be fault-tolerant and low cost
• Complex software free of safety critical errors
• No one “vision” sensor covers all conditions (need RADAR, LIDAR, visual)
• Vision sensor data not completely trustworthy (sun blinding, reflections, fog,…)
• Behavior of other vehicles & pedestrians unpredictable
• Must follow traffic laws, rules of the road
Design of Fault-tolerant Systems
Fail-operational fault tolerant systems

- If simpler solutions (safety mechanisms or simple back-ups) will not serve, fail-op, fault tolerant is needed
  - Loss of function is unsafe, must maintain control despite errors
  - Interruptions unsafe, must provide fast, seamless switchover
  - Immediate repair not practical, must operate safely long enough to obtain repairs
  - Repairs impossible, must design to operate for entire service life without repair
Fault Tolerant Electronics Require Redundancy

- Redundancy needed to provide failure detection
  - Compare the output of two sensors or computers to detect subtle failures
- Redundancy is used to replace lost function
  1. Multiple copies of same design as a back-up
  2. Simpler version of design as a degraded back-up
  3. Dissimilar design for back-up for design errors
- Fault Detection, Isolation and Reconfiguration (FDIR) used to manage redundancy
Space Shuttle used Fault Tolerant Electronics

- 4 identical computers, same software, outputs compared (voted) to detect failure
- 5th Back-up Flight System (BFS) computer with dissimilar software
- BFS could be engaged by crew in emergency
How Can Redundant Systems Fail?

1. Depletion of redundancy
   - Multiple independent failures during mission
   - Latent failure revealed

2. Undetected failure causes a faulty component to remain in control even though healthy redundant units are available

3. A single point failure that effects all redundant components
   - Failure of multiple redundant components from a single root cause (same power source)
   - Failure of one component that cascades to other redundant components (component fails, generates a damaging output)
   - Design error that effects all redundant components (SW bug)
How Redundant System Can Fail Illustration

- **Detect A failure**
- **System is fault free**
- **System operating w/o back-up**
- **System failed**

A & B Fail (single point or common cause)
A & B Fail (depletion)
A Fail (undetected)
B Fail
No Fail

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494 49
Analysis of Undetected First Failure Probability

\[ \lambda = \text{rate of A or B failure (failures / hour)} \]
\[ C = \% \text{ fail detected (coverage)} \]
\[ t = \text{time} \]

Probability (A or B fail) \( \approx 2\lambda t \)
Probability (A and B fail) \( \approx \lambda^2 t^2 \)
Probability (A fail undetected) \( \approx (1-C)\lambda t \)
Numerical Example of Impact of Undetected First Failure

\[ \lambda = \frac{1}{\text{MTBF}} = \frac{1}{10,000} \text{ hrs} = 0.0001 \text{ failures/hour} \]

\[ C = 95\%, \quad t = 1 \text{ hr} \]

Probability (A or B fail) \( \approx 2\lambda t = 2(0.0001)(1) = 0.0002 \) (2 in 10,000) (note)

Probability (A and B fail) \( \approx \lambda^2 t^2 = (0.0001)^2(1)^2 = 1 \times 10^{-8} \)

Probability (A fail undetected) \( \approx (1-C)\lambda t = (1-0.95) \times 0.0001 = 5 \times 10^{-6} \)

Probability (A fail undetected) >> Probability (both A and B fail)

Note: \( P(A \text{ or } B) = 1 - R(A \text{ or } B) = 1 - e^{-2\lambda t} \)

but \( e^{-2\lambda t} = 1 + 2\lambda t + \frac{(2\lambda t)^2}{1!} + \frac{(2\lambda t)^2}{2!} + \ldots \)

So \( 1 - e^{-2\lambda t} \approx 2\lambda t \) for small \( \lambda t \)’s
Fault-tolerant System Single Point Failure Avoidance

- All redundant components must operate independently
- Separate sources of electrical power, cooling, hydraulics
- Physical separation
- Redundancy is electrically isolated, faults are contained and do not propagate (data error propagation must be managed)
- Designed for Electro-Magnetic Interference (EMI) immunity (including lightning, EMP)
- Separation of redundant wiring, avoid common electrical connectors
- Rigorous treatment of design errors (hardware and software)
  - Eliminate by design process
  - Eliminate by test
Typical Fault-tolerant System Design Assumptions

• Multiple independent faults occur sequentially, not simultaneously
  – Much more difficult, costly to design for simultaneous failures
  – Must rigorously eliminate common mode or near coincident failures that invalidate this assumption

• Faults are not “diabolically malicious”
  – Computers will not spontaneously execute complex sequences they have not been programmed to perform
  – However, computers may execute any normal sequence at an incorrect time

• Transient faults (including radiation upsets) may occur more frequently than actual failures
  – Must not deplete system redundancy
  – Result in excessive reconfiguration
  – Distract the crew with nuisance fault indications
Mechanisms for Engaging Back-up Electronics

Primary control

Back-up control

System being controlled
Back-up Electronics – Solenoid Valve

- Primary control
- Back-up control

Provides electrical path for single point failure

Better
- Isolates electronics

Even better
- Ensures flow even if one valve stuck closed (but can’t stop flow if one valve stuck open)

Other solutions use multiple redundant valves in series

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494
Back-up Electronics Controlling a Data Bus

Primary computer fails silent
- Both primary and back-up computers transmit data on the bus
- If primary computer is faulty, it stops transmitting (fails silent)
- Users take primary data if received, back-up data otherwise

Primary computer fails but keeps sending
- Primary continues to send faulty data that appears valid to users
- Primary “babbles” on the bus, preventing the back-up from using the bus

Typically use redundant data bus but this does not solve “babbling” problem
Dual Standby Systems Are Simple, but Problematic

- Back-up switchover requires failure detection (imperfect coverage)
- Switchover mechanism may fail
- Difficult to keep standby channel ready to take-over (state data)
- Standby Channel can be “polluted” by primary channel when primary fails
  - Standby channel state kept consistent with primary
  - Polluted primary state can be transferred before primary fault is detected
Triple Modular Redundancy Uses Majority Voting to Select a Healthy Output

- Voting may be either exact consensus (bit identical) or by approximate consensus (mid value)
- Exact consensus applies to digital signals
- Approximate consensus may compromise coverage
Computer “Voting” Extends the Comparison Idea to Provide Both Detection and Isolation of Faults

Or, in other words, the majority value is correct

A ≠ B and A ≠ C then A is faulty
A ≠ B and B ≠ C then B is faulty
B ≠ C and A ≠ C then C is faulty
Quadruplex Fault Tolerant Architecture

- Quadruplex provides two-fault tolerance
  - Longer duration missions w/o repair
  - Very complex systems where MTBF of each channel is low
  - Need a mechanism to deselected the first faulty channel
A Self Checking Pair Provides High Fault Detection Coverage, Fail Safe Operation

Figure 6.16  Combining failure detection signals using switches.

*Safety Critical Computer Systems* - Neil Storey, Addison Wesley

Tutorial for the 2017 ISSC
Rob Hammett 617-258-2494
Multiple Self Checking Pairs can Provide High Coverage, Fail Operational Fault-Tolerance

- Has greatly improved failure coverage compared to simple dual standby
- But other deficiencies of standby systems remain
  - Switchover mechanism may fail
  - Switchover can interrupt real-time control
  - Difficult to keep standby channel ready to take-over (state data)
  - Standby Channel can be “polluted” by primary channel when primary fails

![Diagram of multiple self-checking pairs](image)

*Figure 6.16* Combining failure detection signals using switches.
Summary – Determining what type of safety approach is needed depends on many factors

- Risks to be mitigated
- Functional complexity
  - Can a simple safety mechanism, back-up or HMI be used?
- Impact of loss of service
  - Is it safe to discontinue service?
- Impact of interruptions in service
  - Time to loss of control
  - Can a man-in-the-loop make the safety decision?
- Impact of transient malfunctions
  - One shot functions?
- Mission duration
  - The longer the system must operate safely, the greater the risk
- Ability to perform repairs
Questions?