Developing Electronic Systems for Safety-Critical Applications

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

- Introduction
- Safety critical electronic controls system examples
- Risks and hazards
- Techniques for the design of safe electronics
- Conclusion
Early Fail-Safe Device – Otis Elevator Safety Brake
Early Fail-Safe Device – Westinghouse Air Brake

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 …
  - Controls functions that if they malfunction could cause harm
  - Controls functions that if they cease to function could cause harm
  - Provides information used to make critical decisions
- 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 control systems without human intervention (drones, self-driving cars, 24/7 monitoring)
• Very precise and efficient control
• Lighter weight, easier to maintain, more reliable than mechanical controls
• Can improve safety
  – Detect and mitigate hazards, including human error
  – 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

*Safety-critical systems must be designed to tolerate defects and design errors*
Electronic Failures – Design Errors

• Software
  – 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, intermittent failures

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 self-clearing, is cleared by cycling power or 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 Accidents

<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 – 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>B2 bomber, Boeing 757, other aircraft lost due to faulty airspeed sensing</td>
<td>Airspeed sensors to electronics blocked by moisture, icing or tape</td>
</tr>
</tbody>
</table>

Countless examples where electronics controls prevented accidents
Fault-tolerant Space Shuttle Electronics Prevented Accident

Fault-tolerance 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
Techniques to Make Electronics Safe

- Fault avoidance (design for high reliability)
- Self-test and status reporting
- 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
  - Testability / self-test / self monitoring
Self Test and Status Reporting

- Embedded computers and software enable self-test
- Electronics designed to compliment the self test software
- Can take different forms
  - Power-on self test
  - Continuous self test
  - Initiated self test (often intrusive)
  - Fault Detection, Isolation, Reconfiguration (FDIR)
  - Mechanical / hydraulic performance monitoring
- Thoroughness (coverage) of self-test a safety consideration
  - Fails to warn user of failure
  - Fails to engage fail-safe or back-up
Human Monitoring and Intervention (HMI)

- **Human monitoring**
  - Typically alerted by system self test
  - Human senses, other data sources, historical knowledge also provide fault detection, isolation
  - Limited reaction times
  - Limited attention span
  - Not present in unmanned systems

- **Human intervention**
  - Cost effective back-up for infrequent events
  - Improvise for unplanned situations
  - Limited reaction time, lack of current situational awareness
Automotive Cruise Control Relies on HMI to be Safe

Function
- Automatically regulate vehicle speed

Consequences of loss of function
- Driver must control, inconvenience

Consequences of malfunction
- Unexpected disengagement
- Inability to disengage
- Unintended acceleration

Probability of malfunction
- Mass produced equipment subject to manufacturing or maintenance induced defects
  - Includes software of moderate complexity

Safety features
- Driver can disengage using brake or on/off switch
- Vacuum servo typically fails disengaged
Automotive Cruise Control – Safety Characteristics

• Interruptions in service acceptable
• No failure detection or alarm provided (human discovery)
• Human overrides to disengage available
• Access & materials to make repairs is assumed available

Presence of an attentive human operator is required to avert hazards
Safety Achieved by Simple Back-up

Two Smoke Detectors

Two Radios in Aircraft

Tutorial for the 2016 ISSC
Rob Hammett 617-258-2494
Safety Mechanism Example – Gas Water Heater

Function
- Turn gas burner on/off to maintain hot water supply

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

Tutorial for the 2016 ISSC
Rob Hammett 617-258-2494

Mythbusters
Gas Water Heater (Continued)

Observations

- Interruptions in service acceptable
- No failure alarm provided (human discovery)
- Access & materials to make repairs is assumed available
- Possible to use two water heaters connected together to prevent service loss (degraded perform – less hot water)

Simple, inexpensive safety features make this dangerous system safe
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

Monitor, Safe mode & switchover control

Primary control

Back-up control

Tutorial for the 2016 ISSC
Rob Hammett 617-258-2494
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
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 2016 ISSC
Rob Hammett 617-258-2494
Advance Driving Assistance Systems (ADAS)

- Iso 26262
- ASIL D electronics
- Throttle
- Brakes
- Steering
- Driver emergency override via mech link

Includes mech link for steering

Multiple Situational awareness sensors

Tutorial for the 2016 ISSC
Rob Hammett 617-258-2494
Advance Driving Assistance Systems (ADAS)

Observations

- Driver inattention makes HMI problematic
- More safety critical than traditional (or advanced) cruise control
- Ability to warn driver of malfunction critical to safety
- Ability to maintain safe control (no fail safe state) long enough (multiple seconds) for driver to take over critical to safety
Steer-by-wire

Function
• Position wheels to steer vehicle in response to electronic command signals from driver (or autonomous driving computer)

Consequences of loss of function
• Deviate from desired path, collision with other vehicles or objects likely

Consequences of malfunction
• Sudden steering changes can result in loss of control, roll over, collision

Probability of malfunction
• Mass produced equipment subject to manufacturing or maintenance induced defects
• Includes software of significant complexity

Safety features
• System must be designed to fail operative and provide warnings of the need for service to restore safety
• Driver can do little other than possibly detect precursor symptoms of impeding failure (if any)
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
All-Electronic Self-Driving Cars

Multiple Situational awareness sensors

Affordable trustworthy electronics

Throttle brakes steering

Humans not expected to take-over in emergency, system must be like fly-by-wire airplane
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
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
A simple, dissimilar interlock not possible – only complex software can correctly initiate.
Risk and Hazards
Safety is Risk Management - Risk Depends Upon Likelihood 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>I</td>
<td>II</td>
<td>III</td>
</tr>
<tr>
<td>Occasional</td>
<td>I</td>
<td>II</td>
<td>III</td>
<td>III</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

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>
Quantifying the Frequency (Probability) of Failures

- Frequent
- Reasonably probable
- Remote
- Extremely remote
- Extremely improbable

Frequency of failure (per operating hour):
- $10^{-0}$
- $10^{-1}$
- $10^{-2}$
- $10^{-3}$
- $10^{-4}$
- $10^{-5}$ (.99999 success)
- $10^{-6}$
- $10^{-7}$
- $10^{-8}$
- $10^{-9}$ (FAA requirement)

Source “Safety Critical Computer Systems” by Neil Story, Addison-Wesley
Examples of Frequency (Probability) of Failures

- **Probable**
  - Frequent: $10^{-0}$, $10^{-1}$, $10^{-2}$
  - Reasonably probable: $10^{-3}$, $10^{-4}$

- **Improbable**
  - Remote: $10^{-5}$, $10^{-6}$
  - Extremely remote: $10^{-7}$

- **Extremely improbable**
  - Extremely remote: $10^{-8}$, $10^{-9}$

**Typical Mechanical parts**
- failure is generally gradual with predictable degradation in performance, preventative maintenance helps.

**High quality electronics**
- failure can be sudden with unpredictable performance, no benefit from preventative maintenance.

**Requires redundancy and fault-tolerant design**

Calculating Probability of Failure

- One or multiple hardware components may fail
  - Component failure rates can be estimated (with much uncertainty) from failure models, historical data
- Software failure
  - No scientific basis for prediction
  - Some relationship to bug discovery rate, complexity
- Cascading or common mode failure of redundant hardware
  - Must be identified during design, eliminated
  - No method for predicting probability

Uncertainty associated with predicting failure probability limits their usefulness in establishing system safety
Examples of Consequences of Failures

Catastrophic
- Loss of life, extreme environmental impact

Critical
- Severe Injury, major environmental impact

Marginal
- Injury, major property damage

Negligible
- Inconvenience, minor damage

Examples
- Plane crash
- Large Explosion
- Chemical exposure
- Oil spill
- Machinery accident
- Non fatal car crash
- 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
Design of safe systems begins with identification of hazards and the functional failures leading to hazards.
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**
- **A Fail**
- **B Fail**
- **A&B Fail** (single point or common cause)
- **A&B Fail** (depletion)
- **A Fail (undetected)**
- **No Fail**

- ○ System is fault free
- 🔴 System operating w/o back-up
- 🔴 System failed

Tutorial for the 2016 ISSC
Rob Hammett 617-258-2494
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

\[ \lambda = \frac{1}{\text{MTBF}} = \frac{1}{10,000} \text{ hrs} = .0001 \text{ failures /hour} \]

C = 95%, \( t = 1 \text{ hr} \)

Probability (A or B fail) \( \approx 2\lambda t = 2(.0001)(1) = .0002 \) (2 in 10,000) (note)

Probability (A and B fail) \( \approx \lambda^2 t^2 = (.0001)^2(1)^2 = 1 \times 10^{-8} \)

Probability (A fail undetected) \( \approx (1-C)\lambda t = (1-.95)*.0001 = 5 \times 10^{-6} \)

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

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

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
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
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

Figure 6.11 A standby spare arrangement.
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

- Computer A
- Computer B
- Computer C

<table>
<thead>
<tr>
<th>Comparison</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>A ≠ B</td>
<td>A ≠ C</td>
</tr>
<tr>
<td>B ≠ C</td>
<td></td>
</tr>
<tr>
<td>A ≠ C</td>
<td></td>
</tr>
</tbody>
</table>

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

Or, in other words, the majority value is correct
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
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
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?