The Patriot Missile Disaster – What Went Wrong?

Liam McBrien, 200309542
Craig McNulty, 200418935
Patriot Missile System Overview

- Mobile missile defence system
- Designed by Raytheon, Hughes and RCA in 1969; produced in 1976 by Raytheon
- Backronym of “Phased Array Tracking Intercept Of Target”
- Initially designed as anti-aircraft system; extended to deter missiles.
How the System Works [1]

• Operates in battalions - usually composed of six batteries
• Each battery has:
  – Radar unit for target acquisition
  – Control station for manual/automatic control
  – Eight missile launchers
  – Communications station
• Targets detected by radar, acquired by control station, and engaged by launchers
Target Acquisition

Figure 3: Correctly Calculated Range Data

1. Search Action - No Range Gate
   Entire Beam Processed

2. Validation Action

3. Track Action - Only Range Gated
   Portion of Beam Processed

Image source: [1]
Target Destruction

- Interceptor detonates in front of target
- Detonation sprays ~1000 pellets forwards in a wide pattern – like a shotgun
- Distance from interceptor to target is important! [2]
  - Ideal range 5-10 metres
  - At 100 metres, probability of hitting target is near-zero

Image source: [3]
Project Timeline [3][4]

- Development started in 1976 as an anti-aircraft system
- First deployment in 1982
- PAC-1 (1988) introduced limited capability against TBMs
- PAC-2 (1990) improved TBM capability
- PAC-3 (2002-) latest version, complete redesign tailored for TBM interception
The Patriot in the Gulf War

• Patriot deployed in the Persian Gulf War to halt ballistic missiles

• Debatable success rate: from Bush’s “97%” to Postol and Pedatzur’s “0%”!
  – What is a “successful” launch?

• January 25th, 1991: ballistic missile hit army barracks in Dhahran, Saudi Arabia
  – 28 soldiers killed, 97 injured
  – Patriot didn’t detect incoming missile
Failure to Launch

Dhahran, Saudi Arabia, 1991
Failure to Launch

- Dhahran protected by six Patriot batteries
- Alpha and Bravo batteries deployed at time of attack to protect Air Base
  - Bravo out-of-commission due to radar problem
  - Alpha running continuously for four days
- Incoming scud missile not engaged by Alpha
  - 28 casualties, more than 90 injured
Software Faults \[1\]

- Patriot computer only had 24-bit precision, so it chopped 0.0001\% off timing values.
- System fell behind by 0.0034 sec (7m) per hour.
- Accuracy threshold is 20 hours.
- System had been running for 100 hours, losing 0.3433 seconds, or 687 metres.
- Range gate affected cumulatively by timing error – looked in the wrong place!
Range Gate Inaccuracy

Figure 1: Incorrectly Calculated Range Gate

Image source: [1]
Code Quality Failure

• Tracking should have depended on elapsed, not absolute time; errors should have cancelled out

• A subroutine which returned a number with 48-bit precision was defined to cope with faster missiles, but was not called in all necessary places \[6\]

• As a result, errors failed to cancel and inaccuracy crept in
Testing Recommendations

• Safety critical code should be subject to heavy scrutiny and reviews, with test cases to ensure numerical accuracy at every essential step
• Program was written in assembly language, which may have presented maintenance and testing difficulties
• Code fifteen years old; lack of understanding, comments, documentation?
• Shouldn’t code safety critical functions at a low level; should abstract away from the hardware as much as possible for safety and testability [7]
Operating Constraints

• Battery intended to run for a few hours per use
  – Poor or non-existent risk analysis?
  – Hangover from old constraints
  – Should start afresh with safety critical systems
    • Registers with 8 more bits give 256 times the accuracy!
• “Very long run times could cause a shift in the range gate, resulting in the target being offset” [1]
  – Supply operators with rich analysis of constraints and limitations to minimise margin of error
• Rebooting to reset state
  – Downtime produces a 90 second window of vulnerability; power cycling should be a last resort
Safety By Diversity

• Essential for safety critical systems
• Several instances of single points of failure
  – No early warning from observation system in Narrungar, Australia \(^{[8]}\); though expensive to maintain, should other such systems be available? \(^{[9]}\)
  – Other battery was broken - two batteries with a “run for three hours at a time” constraint is a lethal combination - three hour repair window!
  – Updated software arrived the next day \(^{[10]}\); should delivery have been expedited? Perhaps have software engineers on site?
Patriot Accuracy

... or inaccuracy?
Accuracy Claims

• George Bush Snr claimed 97% success:
  – “Patriot is 41 for 42: 42 Scuds engaged, 41 intercepted!” [11]

• U.S. Army claimed initial success rate of 80% in Saudi Arabia and 50% in Israel
  – Later scaled back to 70% and 40%

• 1992: Postol and Pedatzur testify that according to their studies, success rate closer to 10% and perhaps even 0% [3]
What is a ‘Successful Launch’?

• Standard practice: fire four Patriots at each incoming Scud
  – 25% accuracy should result in around 100% success rate

• What is a ‘kill’?
  – Hitting the warhead?
  – Hitting the missile?
  – Deflecting the missile?
Observed Misses

• Postol (1992) documented misses observed through press footage
• Patriots often missed target by >100m
  – Range gate errors?
  – Late launches – ‘early warning’ failure?
• Patriots dove into the ground
  – Rocket motor failures?
• Scud breakup caused incorrect targeting
  – Hull debris targeted rather than the warhead
Possible Reasons for Inaccuracy

- Errors in prediction and tracking: holdovers from the retrofit to track TBMs?
- Missile failures: inadequate field testing?
- Targeting the wrong part of the missile:
  - Iraqi redesigns caused Scuds to be faster but more prone to breakup\(^{[11]}\)
  - Software needed faster response to changing operational parameters (or more adaptability)
Project Management Faults
Customer Focus

• System designed without contemplating stakeholders – operators/soldiers!
  – Should ensure that a customer (or proxy) with field experience is available
  – User acceptance tests verified by customer

• Retrofitted to run in unfamiliar context
  – Simulations or mockup exercises with potential operators
External Pressures

• Taxpayers money – project managers may have prioritised dollar over human cost
  – “Value of human life” perhaps had an impact; dire history, e.g. the Ford Pinto$^{[12]}$
  – “We can just patch this old system up” attitude

• Rushed rollout – pressure from customer to deliver software
  – Requirements non-negotiable – testing suffers
Safety First

• Project management’s top priority should have been maximising safety
  – Testing should extend beyond ‘normal operational parameters’ and be supported by software
  – Definition of abilities and limitations must be clear and explicit
  – No ‘single points of failure’ can be tolerated
  – Critical vulnerabilities must be identified and fixed as quickly as possible
  – Instead of delivering faulty software on time, fully operational software later could have given the best outcome
Outcome – PAC redesign

- PAC-3 (current version) designed ‘from scratch’
  - Learning from Desert Storm mistakes
  - Much higher success rate in Iraqi Freedom: 9/9 kills (8 confirmed, 1 probable) \[^5\]

- MEADS (next version) learning from Iraqi Freedom mistakes
  - IFF improvements to reduce ‘Friendly Fire’ incidents
References


References


References


References

