FMECA AN UNDERUTILIZED TOOL

Daniel Mullin B.Eng, Hardware S&MA
Canadian Space Agency

May 23, 2013

How and why is it underutilized?

- Often started too late
- Since it often isn't performed to full potential it's usefulness is undermined
- Many program managers and systems engineers don't realize how powerful it is
- Not deemed as critical for unmanned missions
- Lots of heritage technology reuse
- Program cost pressure

Purpose of the FMECA

- SPFs
- Catastrophic, LOF, hazardous SPFs need to be identified and communicated to all stakeholders

EARLY! EARLY! EARLY!

- Design changes forced by SPFs can be extremely expensive
- SPF avoidance is key design driver in most cases, even nature abhors an SPF

Credible or not?

- Failure modes must not be overlooked or dismissed offhandedly
- Even more important with development of autonomous and script based systems
- Malicious computer or Byzantine General

Hidden Redundancy

- SPFs can be mitigated through Degraded modes of operation
- Operations engineers and mission designers need to understand system behaviour and their options
- Work arounds may include both software and hardware options

To be redundant or not that is the question?

- What to do in the face of catastrophic or critical failure modes?
- How fault tolerant do we need to be?
- System redundancy is major system design decision
- Major program driver of:
  - Cost
  - Schedule
  - Verification and testing

What's Missing?

- Latent failure modes are often not well understood or included
- Dormant or cold redundant subsystems must be analyzed for latent failures
- How do these failures affect fault tolerance?
- How do you switch from one string to the next
- Need to eliminate latent failures can have major design impacts.

Scotty, seconds not minutes!

- Time to effect, detect and correct
- Time based failure analysis can be vital to operations and mission planning
- Can impact or change the criticality of a failure
- ROM estimate is usually sufficient for FMECA

The computer made me do it!

- FMECA must include software failure modes
- Also operator error
- Inadvertent commands can often be catastrophic
- FMECA provides important input for software design and V&V
- Fault messaging and injection will impact system design

Where's my RPN?

- Frequency, severity and….?
  - Likelihood of detection
  - Time based analysis
- Provides a method for quantitative evaluation and ranking of Risk
- Useful as an at-a-glance reference for all stakeholders

CIL

- Usually included
- Important program tool
- Direct impact to program cost
- Critical software needs to be included

Thank-you

- MIL-STD-1629 states, “A properly performed FMECA is invaluable to those who are responsible for making program decisions regarding the feasibility and adequacy of a design approach”
- Questions?