RAMS – Is That When You Have More Than One Sheep ?

PYB Consulting

PYB Consulting

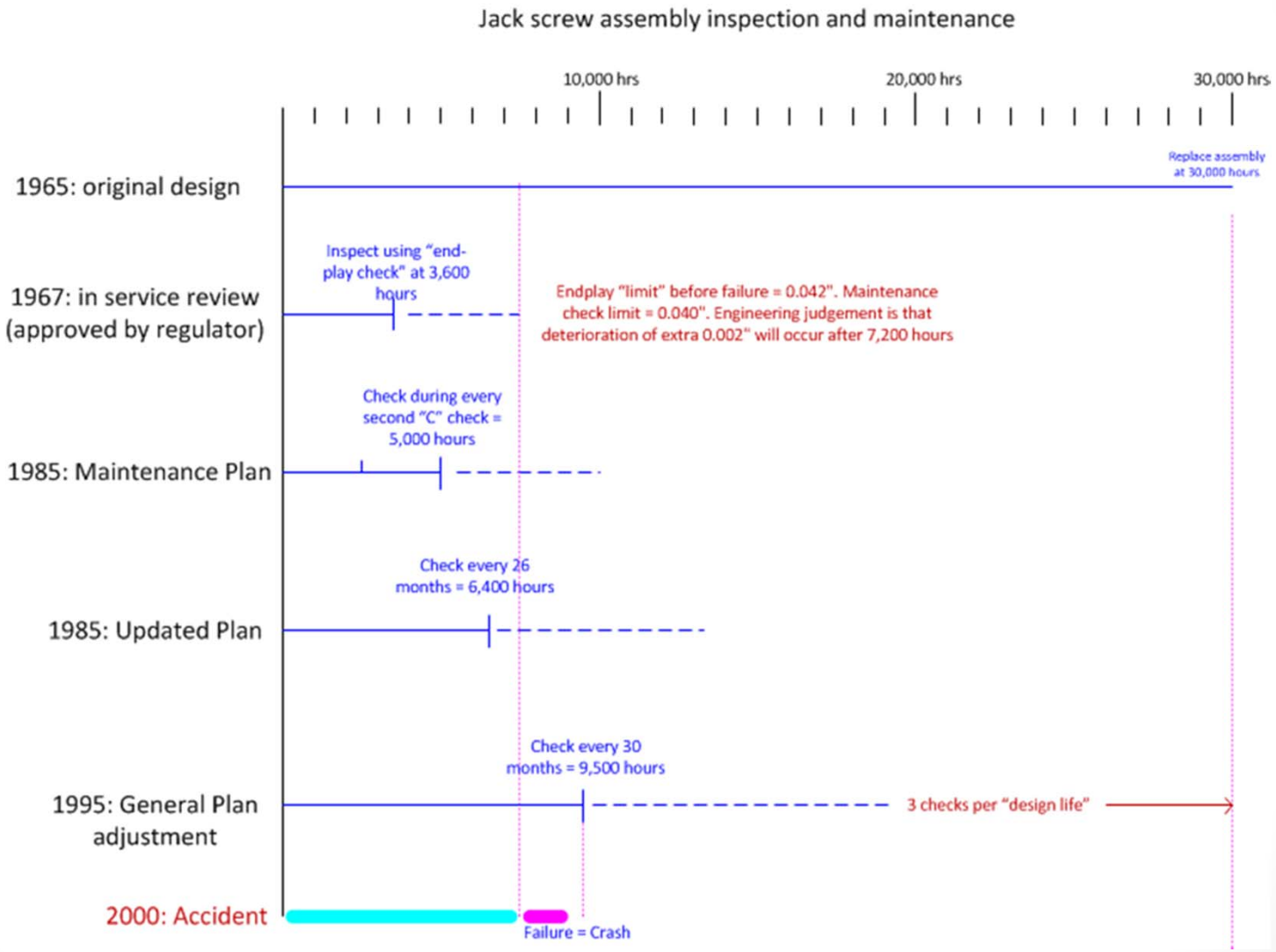
Elements of Systems Engineering

- **Tombstone technology – the paradigm**
  - The old ways
  - Alaska flight 261
- **RAMS – Some low hanging fruit**
  - Tri-colour signals.
  - Fixed train stops
- **Why is this important?**

The Traditional Approach

- **Tombstone technology**
  - Learning comes primarily from past accidents
  - Special controls named after accidents
  - Controls become recyclable ("Stop" signs)
- **Training "on the job" by "experienced practitioners"**
  - Heavily reliant on the quality of the experienced practitioners
  - Competence assessed based on time spent rather than knowledge or outcomes
  - Thin objective knowledge base
  - Risky to introduce innovation
- **Consequence of getting it wrong**
  - You cannot change what you do not understand
  - Alaska flight 261
  - Crash killed all on board

Alaska Flight 261

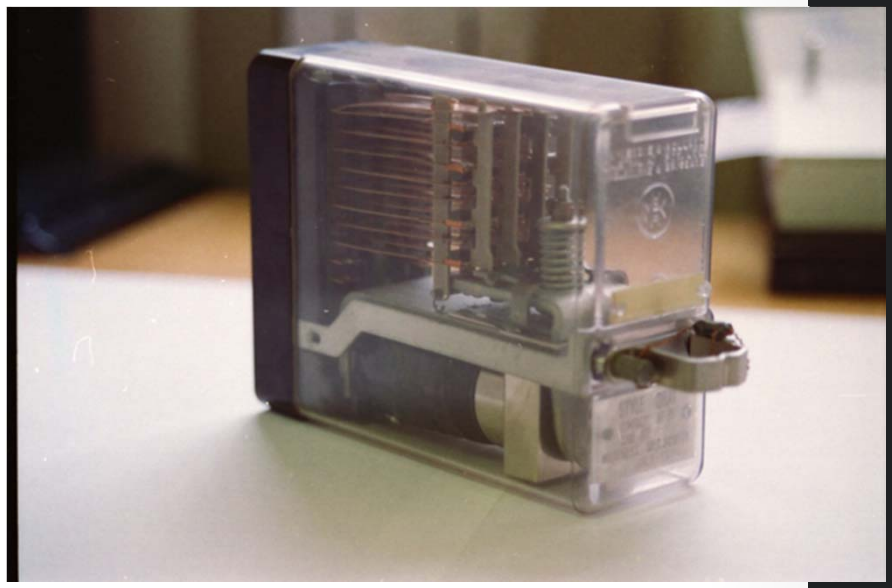


A Better Way

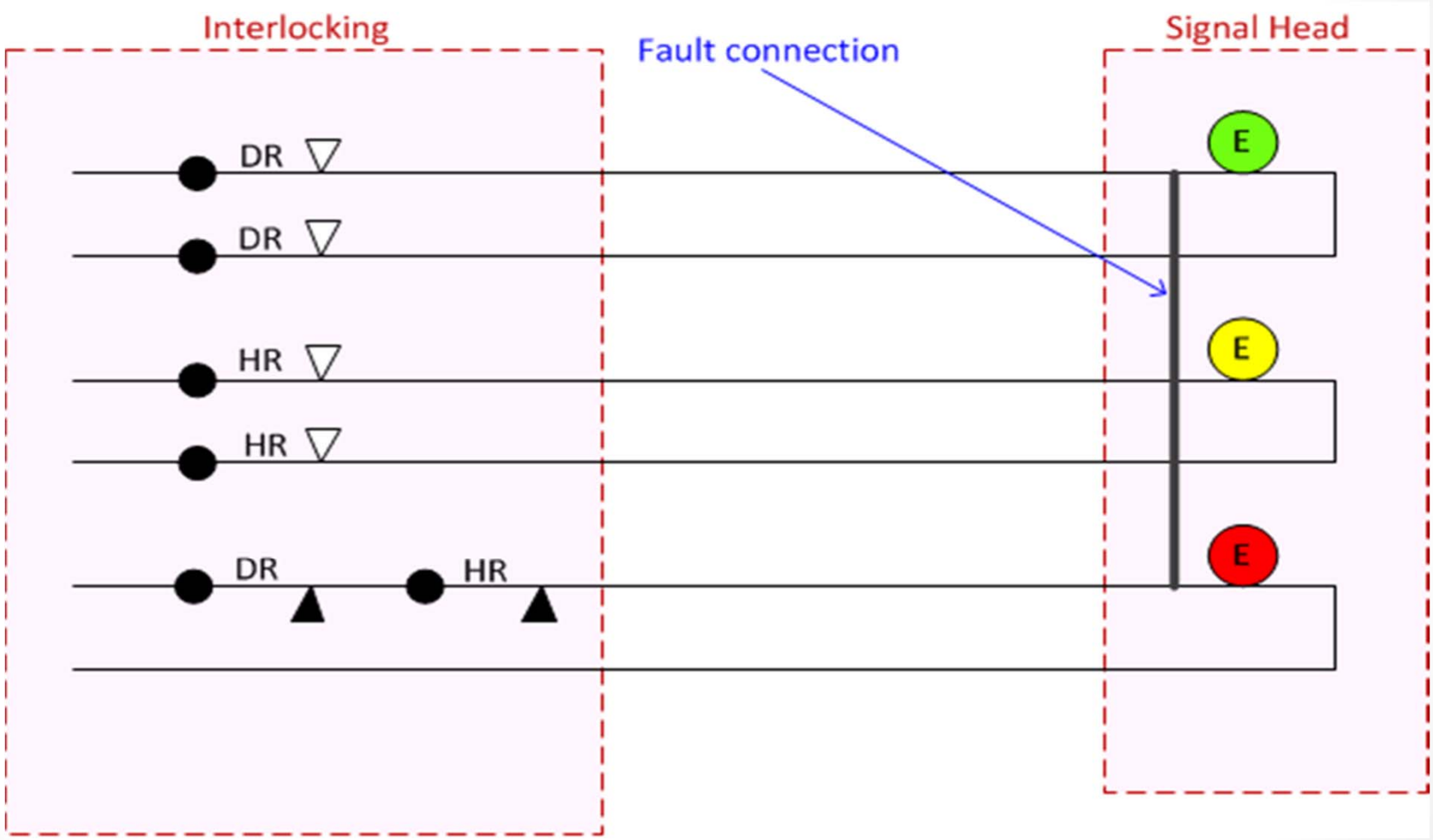
- **RAMS: Policy based on knowledge based analysis**
  - Emphasis on solid detailed understanding of failure modes and rates
  - FMECA approach drives engineering
  - Focus on system interfaces
  - Provision of facilities to publish:
    - Historic failure rate data
    - FMECA models and data
    - Studies into fundamentals
  - Standards based on common foundation of engineering knowledge
- **Accidents no longer required**
  - Technology change underpinned by analysis
  - FMECA can lead service experience
  - Value added at system interfaces

RAMS: Tri-Colour LEDs

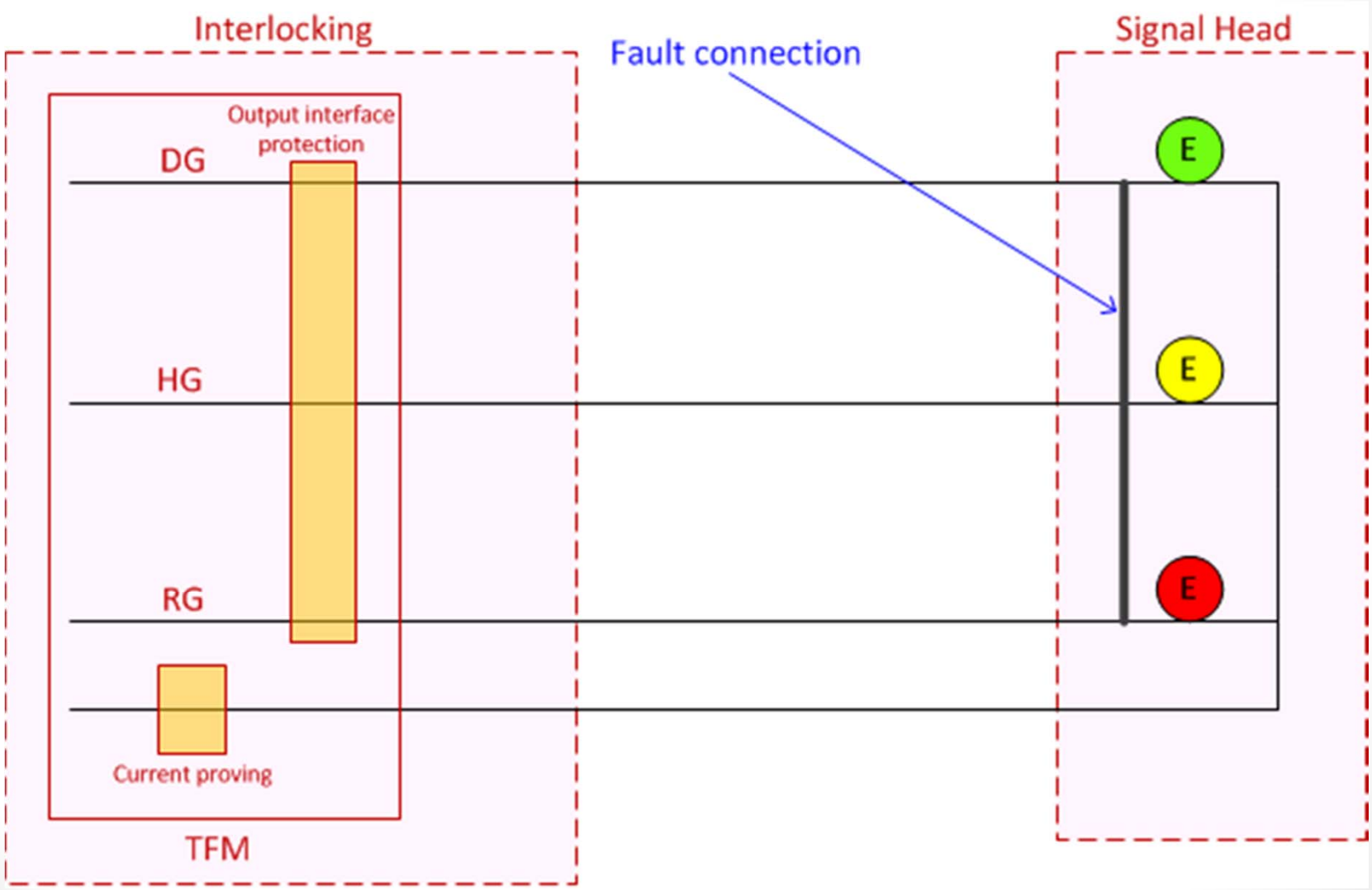
- **"S" is for "safety"**
  - SIL-4 analysis includes assumptions about interfaces
  - Total system safety is not guaranteed by using SIL-4 components
- **LED module failures**
  - Traditional safety assured by circuit isolation and double cutting
  - SSI utilises "Output Interface" protection instead
  - Benefits to LED suppliers and users
  - SIL-4 safety assurance assumes SSI interface protection
- **Examples of interfaces**
  - Adjacent subsystem
  - Environment or inter-discipline system
  - Maintainer
  - User



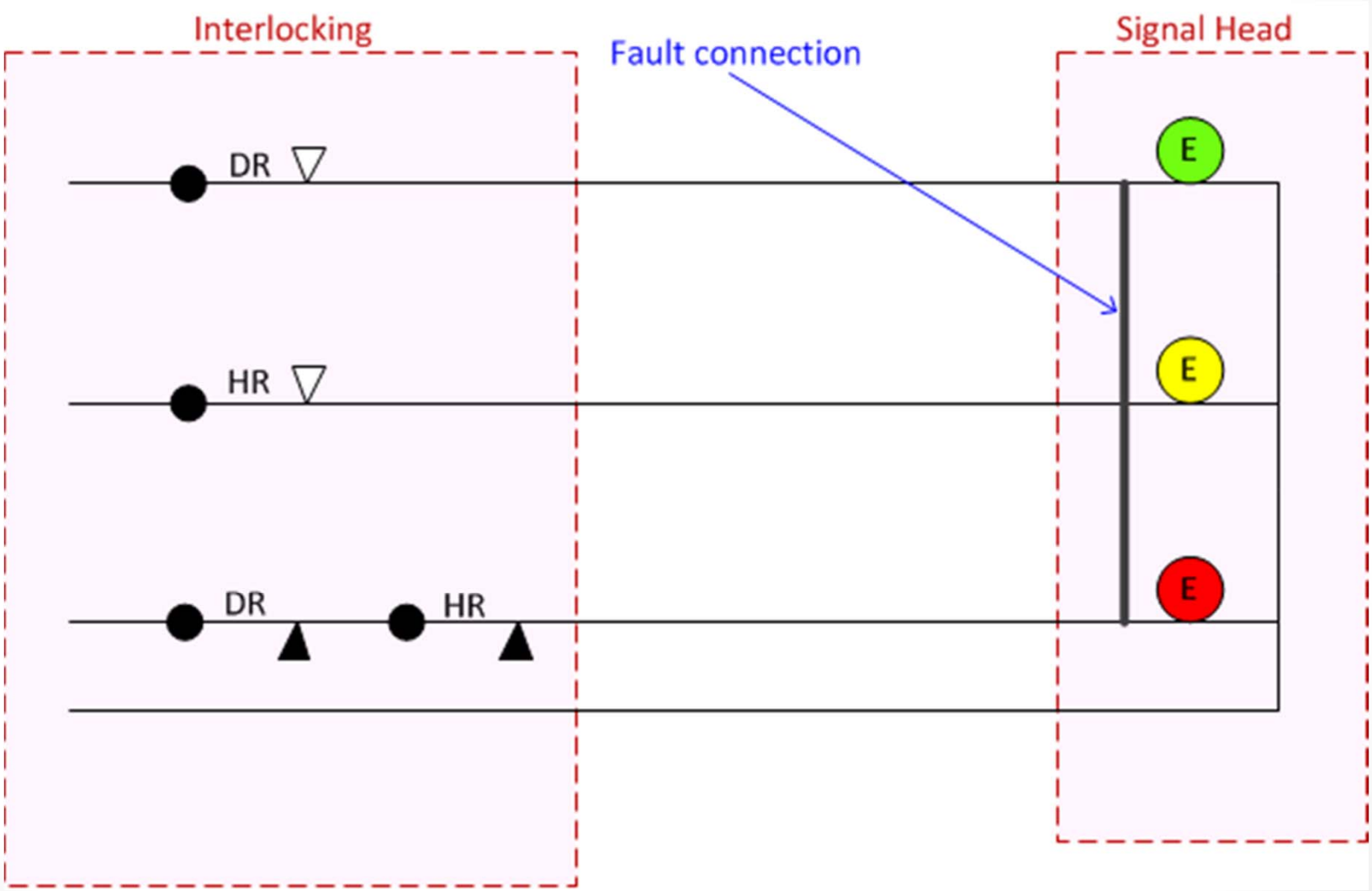
LED Signals – Traditional Relay



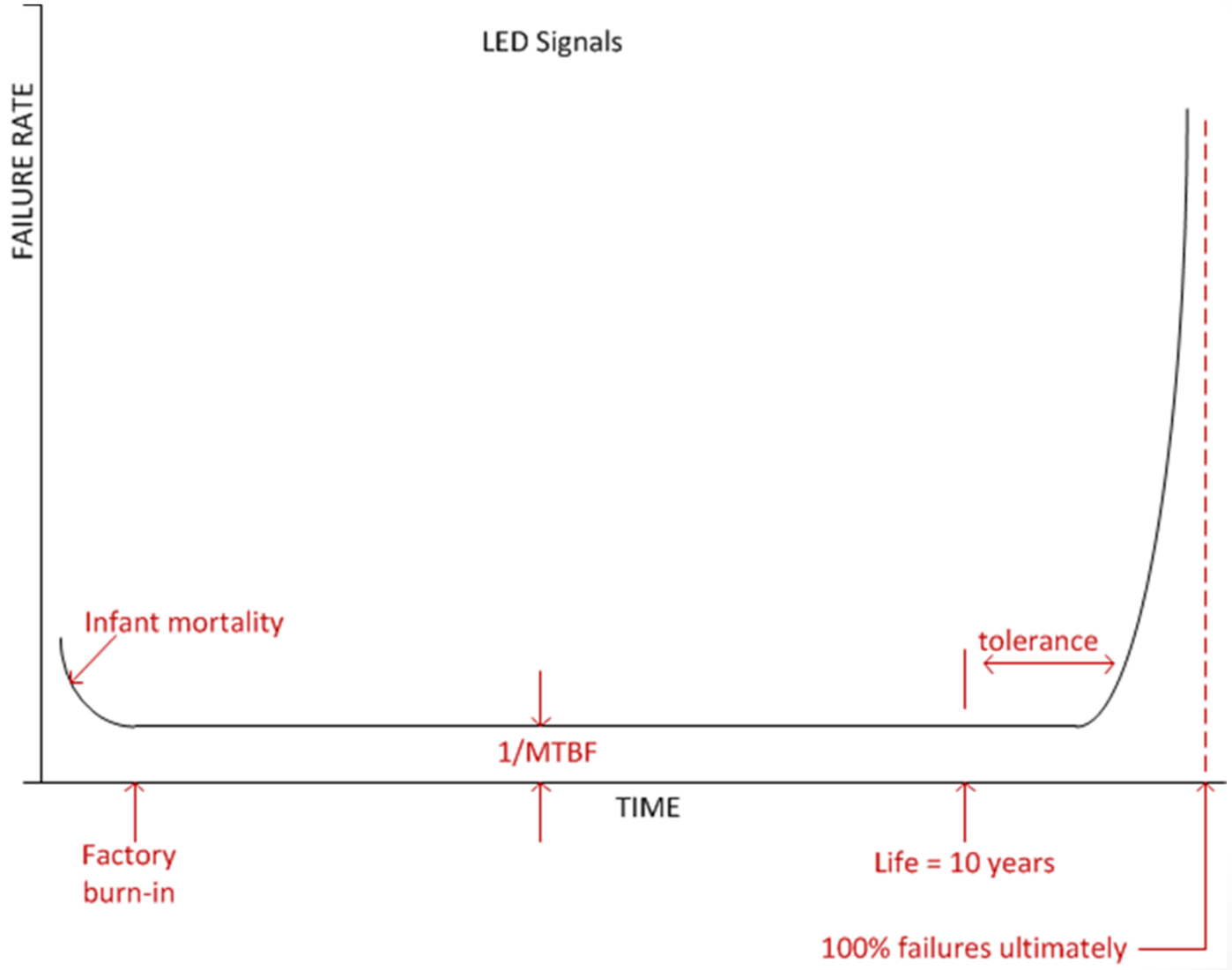
LED Signals – SSI Implementation



LED Signals – Failure Risk



LED Signals – Failure Mode



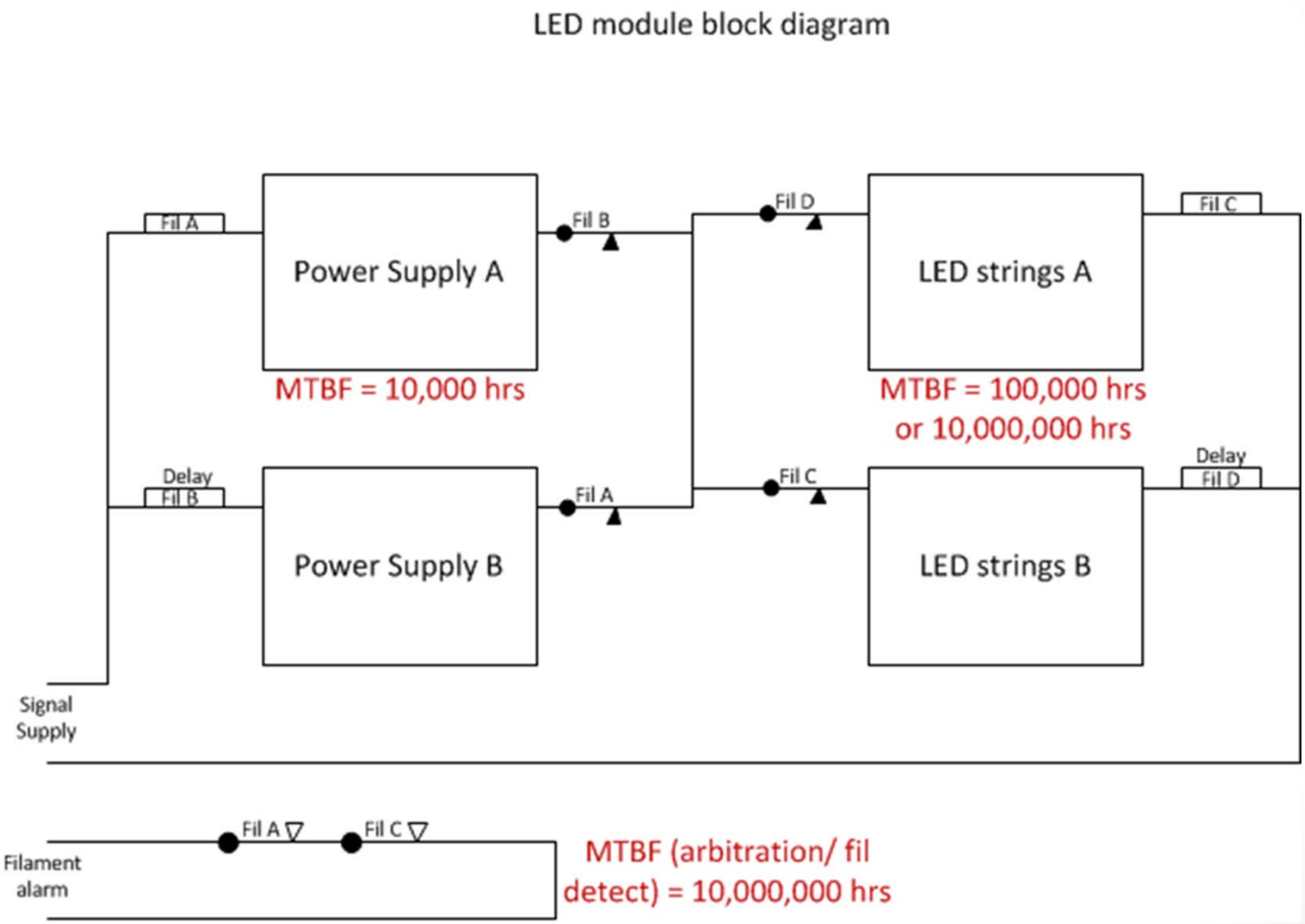
RAMS: LED Signals

- **"R" is for "reliability"**
  - Reliability is an outcome of:
    - Equipment characteristics,
    - Environment; and
    - Maintenance policy
  - Supplier only controls dot point 1
- **Bath tub curve may apply**
  - Cars have bearings, but failures are rare
- **LED signals**
  - Supplier quotes "life data" as MTBF
  - What is mid-life MTBF?
  - Is data available?
  - Studies could add value

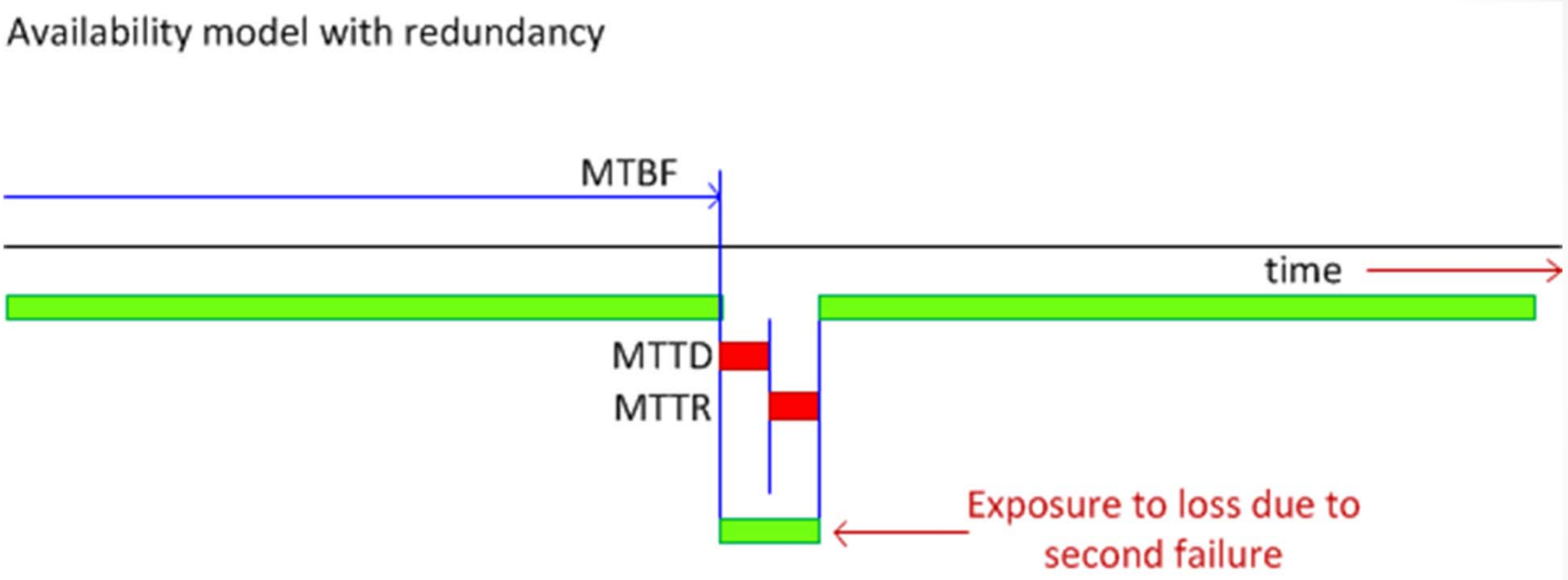
RAMS: LED Signals

- **"A" is for "availability"**
  - Availability is an outcome of:
    - Requirement
    - Reliability
    - Redundancy; and
    - Maintenance policy
  - Supplier only controls part of dot point 2
- **LED signals**
  - Signal must display aspect to driver
  - Signal number must be identifiable
  - More availability can reduce reliability
- **"M" is for "maintainability"**
  - Maintainability is an outcome of:
    - Equipment design
    - Maintenance policy
    - Environment
  - Supplier and IM must consult

LED Signals – Model Configuration



Safety With Redundancy

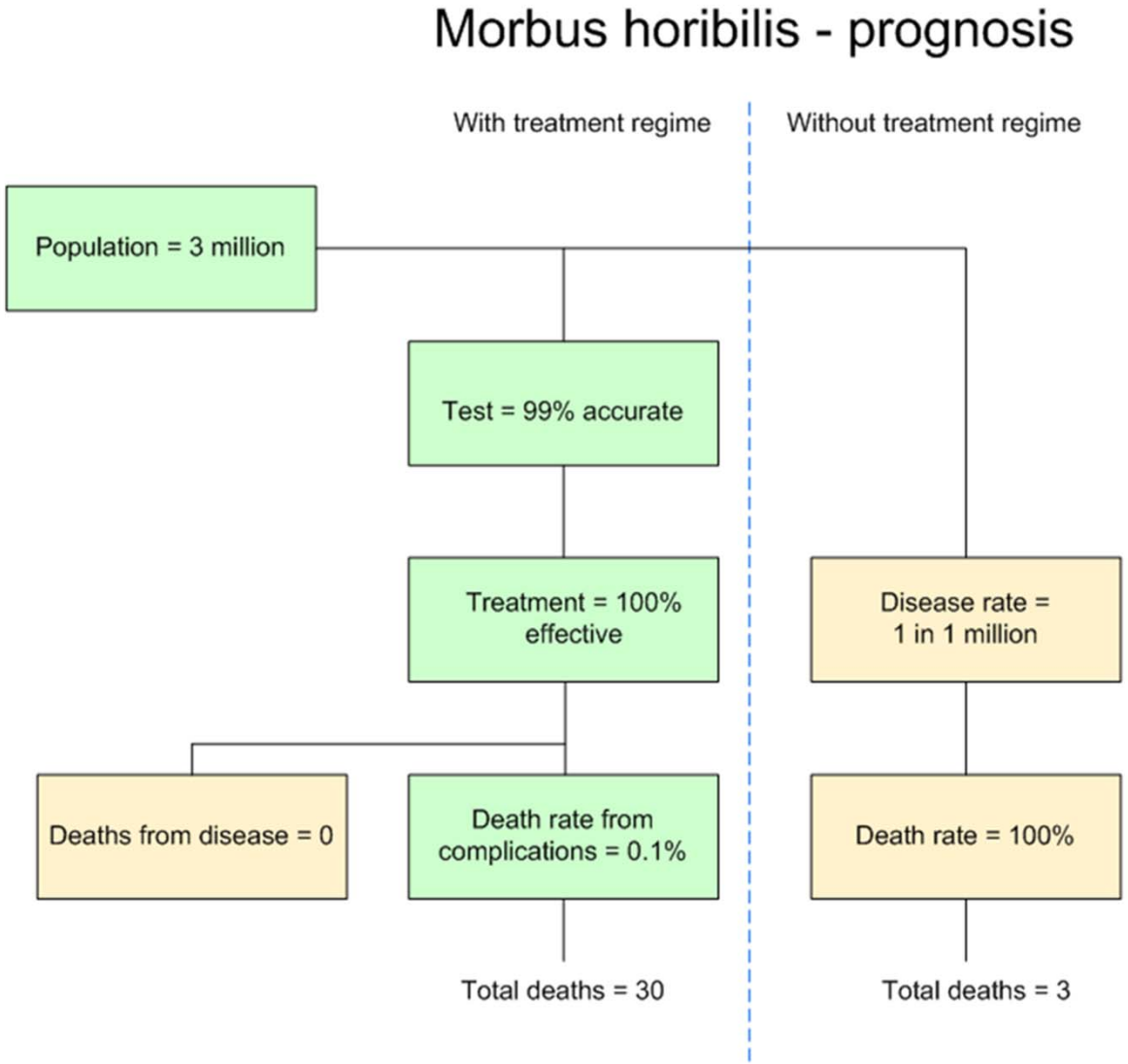


PYB Consulting

RAMS: Fixed Train Stop

- **"A" is for "accident"**
  - Tombstone technology in action
  - Current policy is a result of
    - Runaway from Broadmeadows
    - Inadequate detection/response regime
- **Prior practice**
  - Presence detected by inspection
  - Replaced when reported missing
- **Revised practice**
  - Adjustment detected electrically
  - Attendance by maintainer enforced
    - Approach signal set to stop
    - "maintainer will not attend otherwise"
- **Is safety improved?**
  - Need to consider new risks created

Safety With Redundancy



Rail Case

- **Accident scenario**
  - Signalling “Right Side” failure
  - Train sees signal at stop and stops
  - Driver applies the rules to pass the signal and proceed forward
  - Train collides with train in section
- **Noted cases**
  - Glenfield (NSW – 1999)
  - Craigieburn (Vic – 2010)
  - Holmesglen (Vic – 2000)
  - Aircraft (Vic 1999)
  - Syndal (Vic 1989)
  - Ringwood (Vic 1989)
  - South Dynon (Vic 1986)

Our Responsibility

- **Responsibility of experts**
  - Sheppard J:
    - "… *the court will nevertheless take into account evidence given by persons experienced in the particular profession involved as to standards which are considered appropriate within a profession*."
  - Hochfelder v Ernst & Ernst:
    - "… *we are not constrained to accept faulty standards of practice otherwise generally accepted in an industry or profession*."
  - There is a need for a profession to ensure that standards are "up to date" and have taken account changing circumstances and technology

- **"S" is for "studies"**