IRSE

Institution of Railway Signal Engineers

Dependability of Railway Control & Communications Systems version 4

An introduction for candidates taking Module A of the IRSE Professional Examination

Hedley Calderbank FIRSE

Dependability

- Composed of 4 elements (giving the RAMS acronym):
  - **R**eliability - the probability that the item will deliver its required function when required.
  - **A**vailability - the proportion of time for which the item is in a state to perform its required function.
  - **M**aintainability - the ease with which an item is kept in working order or repaired.
  - **S**afety - freedom from unacceptable risk of harm.

Security is sometimes considered separately and cuts across the 4 elements above.

Maintenance

- Once the system has been designed, installed and tested, MAINTENANCE is the process that keeps the system DEPENDABLE. It can consist of processes such as visual inspection, adjustment, lubrication, renewal of parts, testing.
    - Preventive Maintenance - to keep the item safe and reliable (usually on a pre-determined schedule).
    - Predictive Maintenance - preventive maintenance that is only done when the item is predicted to fail or become unsafe (e.g. from remote condition monitoring data).
    - Reactive (or Curative, or Corrective) Maintenance (or Repairs) - restoring the item to working order once it has failed or has a defective part.
    - Renewals – Replacing items before they become worn, unreliable or unsafe.

preventive maintenance is usually most valuable on items with moving parts in a severe environment (e.g. points machines)

Reliability

Reliability

- The probability that the item will deliver its required function when required.
- Delivery of correct functions when in service (Will it work when it is needed?)

- Often measured as Mean Time Between Failures (MTBF). This formula gives a good approximation
  - MTBF = Length of Time / Number of Failures in that time
  - e.g. At population level, for 120 items, there are 50 failures in a year. The average MTBF for an individual item is 120/50 = 2.4 years.
- This will typically be measured in years for elements of a railway system (e.g. radio transmitter, track circuit), but lower for whole systems.
- MTTF (Mean Time To Failure) is a very similar measure used for non-repairable systems

Some causes of poor Reliability

- Poor design (e.g. software bug, component not resilient)
- Maintenance issues not considered at design stage (cost or time pressure?)
- Poor build or installation (e.g. “nicked” wires, stripped insulation, inherent weaknesses)
- Poor maintenance (e.g. weakness or fault left after last intervention, deficiency not detected at last routine test or visit)
- Abusive operation
- External (e.g. severe weather, power outage, physical damage, electromagnetic interference)
- Electronics affected by the tough rail environment
- Failure to learn from past failures !

Examples of root causes of poor Reliability

- Track circuits *(with typical symptoms)*
  - Flooded or contaminated ballast *(track showing occupied when clear, or variation in test readings)*
  - Poor insulation of track fixings *(track showing occupied when clear)*
  - Failure of Insulated Rail Joint (IRJ) *(track showing occupied when clear)*
  - Railhead contamination *(failing to detect a train)*
- Points *(with typical symptoms)*
  - Unstable track *(loss of detection – intermittent or permanent)*
- Lineside equipment
  - Electromagnetic interference
  - Vibration
  - Temperature
  - Humidity

Examples of Good Reliability

- A highly **reliable** signalling system:
    - Will ideally never fail (though may have internal faults or deliver degraded outputs)
    - Will self-diagnose internal faults before they cause a failure of the system (e.g. remote condition monitoring)
    - Will cope with the real world railway operating environment (both normal and abnormal)
    - Few single points of failure
    - Will cope with possible failures in other systems (e.g. power supply failures or minor interruptions)

Availability

Availability

- The proportion of time for which the item is in a state to perform its required function.
- Continuity of correct service (For how much of the time is it usable?)

At its simplest if can be expressed as:

Availability = Uptime / (Uptime + Downtime)

This is the equivalent of:

Availability = MTTF / (MTTF + MTTR)

Where MTTF is Mean Time to Failure (or use MTBF instead)
and MTTR is Mean Time to Repair (from time of failure to rectification).
Planned outages need to be counted as failure incidents

This will typically be nearly 100% for most items of railway equipment, but lower for whole systems. Any unplanned system availability less than 100% causes loss and customer dissatisfaction.

Some effects on Availability

Negative

- Intrusive preventive maintenance
- Taking system out of service (planned)
- System out of service because of failure
- Restricting train movements to safeguard staff

Positive

- Duplication of system components or back-up systems *(can increase availability without component reliability being increased)*

Examples of Good Availability

- A highly **available** signalling system:
  - will work 24/7 (or all traffic hours)
  - any maintenance routines do not need the system to be taken out of service
  - will continue to deliver at least minimum functionality in the events of faults
  - fault rectification does not need the system to be taken out of service
  - does not require any work on the lineside

Maintainability and some issues affecting it

Maintainability - the ease with which an item is kept in working order or repaired.

- Weather protection for maintenance staff
- Ergonomics
- Easy or zero maintenance routines
- Workflow on mobile device
- Diagnostic tools to quickly identify cause of failure
- Remote testing, configuration & faulting
- Modular replacement (especially on failure)
- Obsolescence (parts, skills, support)

Good Maintainability

- A highly **maintainable** signalling system:
  - Ideally needs no routine maintenance
  - Otherwise, wherever possible, requires routine maintenance which aims ideally to be:
    - Minimised
    - Easy to do, using normal tools and test equipment
    - Not very highly skilled
    - Non-disruptive (e.g. can be done while trains run)
    - Not on or near the track
    - Remote (at central staffed point, or via internet from anywhere)
  - Is quick to repair (easy access, modular, diagnostics)
  - Has lifetime access to spares and technical support

Safety

Safety - freedom from unacceptable risk of harm.

This includes:

- System Safety – the ability of the control and communications system to protect train movements at all times (including the associated design, installation, maintenance and operating processes & practices).
- Staff Safety – not exposing people who maintain, operate or install control and communications systems to danger or harm (including signallers, drivers, operating staff as well as maintenance and installation technicians)

Some issues affecting System Safety

- Interlockings – designed, installed and tested to be safe in all combinations of circumstances
- Colour light signals – visible in all conditions
- Points – locked, detected & maintained correctly
- Train detection – no false clears with a vehicle present
- Axle counters – assurance of clear track before reset
- Cables – no false feeds or earths
- Indications – failures can mislead operators or deny them critical knowledge
- Hardware & Software – designed to fail safe, or (better still) to degrade gracefully & safely

Maintenance Errors can cause Unsafe Conditions

- The following help to avoid errors
  - Easy-to-follow maintenance instructions
    - Avoid the need to refer to a large manual
    - Encapsulated checklists or prompts on mobile devices are good
  - Staff training
    - Acquiring the necessary skills
    - Avoiding the need for frequent reference to maintenance instructions
  - Staff competence testing (at regular intervals?)
  - Design to make errors difficult (e.g. pin coding of plug-in modules, plug couplers to prevent a wire being connected to the wrong circuit)
  - Maintainability issues (e.g. ergonomics, weather protection)

All the above are better than the threat of disciplinary action after a mistake is made.

Safety

- A **safe** signalling system:
  - Prevents collisions and derailments
  - Conveys clear instructions to drivers
  - Fault tolerant (or degrades gracefully) so manual movement authorities or workarounds are avoided
  - Fails safe where complete failure is unavoidable
  - Has software designed to default to the safest state
  - Uses plug-in modules that are colour-coded (good) or pin-coded (better) to prevent use of the wrong module
  - Does not expose staff to danger (e.g. trains, high voltages, hazardous environments)

Impact on Safety of Reliability & Availability

Why will a signalling system with poor reliability or availability worsen safety?

Because the signal operator will have to use manual procedures more often to allow trains to run.

Being open to human error (and not fully protected by the fail-safe design of the signalling system) manual procedures are inherently less safe.

Security and some issues affecting it

Security

- o Protection against external actions or events (usually confined to malicious ones)
- o Will it work without being degraded by changes or disruptions?

- Cyber security
- IP enabled systems
- Theft
- Vandalism
- Insider threats

Good Security

- A highly **secure** signalling system:
  - is immune to all forms of cyber attack
  - is resistant or unattractive to theft
  - is resistant or unattractive to vandalism
  - has protections against malicious actions by insiders

Examples of how to Improve Dependability

- Technology
  - Axle counters eliminate insulated block joint failures and track circuit failures from flooding or rail contamination.
  - ETCS - can eliminate signals and track circuits
  - LED signal lamps - longer life and fewer failures
- Redundancy
  - Eliminate single points of failure
  - Overlap radio coverage
  - Duplicate electronic interlockings and lineside modules
- Improve MTBF (Mean Time Between Failures)
  - Design and install equipment for high reliability
  - Reduce environmental stress (e.g. cooling)
  - Improve the preventive maintenance regime
  - Introduce remote condition monitoring

RAMS Tools for improving Dependability (1)

FMECA (Failure Modes, Effects, and Criticality Analysis)

A methodology to identify and analyse:

- all potential failure modes of the various parts of a system
- the effects these failures have on the system
- how to avoid the failures and/or mitigate the effects of the failure on the system

RCA (Root Cause Analysis)

- A method of problem solving used for identifying the root causes of failures and displaying them graphically (e.g. Fishbone or Ishikawa diagram)

RAMS Tools for improving Dependability (2)

CCF (Common Cause Failure analysis)

- Identifying all the ways in which a single fault can cause a system failure, even where system components are duplicated to improve reliability. Statistical analysis then allows a meaningful system reliability figure to be calculated.

FTA (Fault Tree Analysis)

- To identify the best ways to reduce the risk of a system failure by tracking the various sequences of events that could lead to the failure.

DRACAS (Data Reporting And Corrective Action System)

- Tracks all failure related data throughout the period from manufacturing to in-service

RAMS Tools for improving Dependability (3)

FRACAS (Fault Reporting, Analysis & Corrective Action System)

- Process for reporting and analysing failures, then planning corrective actions. FRACAS records the problems related to an item and their associated root causes to assist in identifying corrective actions. Fault Control desks would use this.

RCM (Reliability Centred Maintenance)

- Optimises the frequency and scope of preventive maintenance interventions to reduce failures and their impact on railway operations. It takes account of factors such as:
  - Typical failure modes
  - Probability and consequence of failure
  - Safety risk
  - Performance risk
  - Number of operations
  - Operating environment

Improving 'Wear-out'Period Reliability

- Optimising Maintenance & Renewals:
  - Understanding impact of Failures on Safety & Performance (FMECA based)
  - Collecting key asset information for reliability analysis
  - Determining Asset Life Characteristics (point of onset of increasing failure rate)
  - Checking current and future availability of spares and technical support
  - Using all the above to inform the maintenance & renewals policy (i.e. when should we renew? should we change the maintenance regime?)

Dependability Measurement
(Operations Phase)

A few examples:

- Mean Time Between Failures (MTBF)
  - = Length of Time / No. of Failures during that time
    - Also MTBSAF for service affecting failures
- Number of Signalling Failures (or those causing delay, or safety risk)
- Mean Time To Repair (MTTR)
  - (from time of failure to rectification)
- Downtime costs
- Consider leading indicators e.g. staff competence, asset condition

Digging Deeper than System Failure Rate

- Capturing all relevant data at component level (e.g. points, track circuits, radio aerials) gives the best opportunity for Dependability improvement
  - Fault rate
  - Precise cause
  - Environment
  - Fault history of component (use Computerised Maintenance Management System – CMMS)
  - Maintenance history of component (CMMS)
  - Asset condition

- Data consistency is challenging. Different people will code the same failure, or event differently unless the data coding structure is simple and foolproof.

Remote Condition Monitoring

- Predictive Maintenance is the ideal to aim for (i.e. detecting a potential fault before it happens – and early enough to fix it before the system fails)
- Data should be transmitted to a person who can take prompt action
- Examples:
  - Points slow to operate
  - Error rate on data link
  - Signal lamp filament failure
- But not possible for all railway control & communications equipment

Conclusions

- Dependability is hugely important (impact on whole life costs).
    - Operations and maintenance (including cost of failures) usually exceed the capital cost of a system over its lifetime
    - “Does it work?” “Is it safe?” are not enough for a project to aim for
- Design for Dependability
    - Much cheaper and more effective than retro-fitting
    - Don’t let it be value-engineered out of scope
    - 40 years system lifetime of regret, if you get it wrong!
- Focus on Dependability throughout operational lifetime
    - Use measurement and analysis