

# Reliability & Maintainability Design Aspects of Signaling Products and Systems

by

Chinnarao Mokkalpati, Union Switch & Signal Inc.

Jim Hoelscher, Safetran Systems Corp.

AREMA C & S May 23, 2006

# Introduction

- Signaling Supply community follows elaborate processes to provide safe and reliable products
- Safety processes have received a lot of attention
  - AREMA C&S Manual Parts 17.3.1, 17.3.3, 17.3.5, 17.5.3, 17.6.1
- Reliability processes are less publicized
  - AREMA C&S Manual Part 17.4.1

# Purpose

- Provide insight into the processes followed by signaling design and supply community to achieve reliable and maintainable products
  - Hardware and software reliability, maintainability and availability design and test processes are explained.

# Why Reliable & Maintainable?

- Cheaper to make reliable products than to make unreliable ones
- Unreliable products
  - failure costs and warranty = 5% to 10% of sales
  - Loss of credibility and reputation
- Reliable products
  - 4% to 5% of sales

# Hardware Reliability

- Parts with broad usage base are used (new, single industry usage parts are avoided).
- Parts with 'reliability' history are used.
- Parts available from multiple suppliers with various levels of quality screening are used.
- Modular design techniques are used:
  - For maintainability
  - For part obsolescence management.

# Hardware Reliability

- Temperature is the most significant factor affecting reliability.
- Failure rate increases as a function of temperature and stress
  - A transformer operating at 85 C has a failure rate that is 27 times the failure rate at 40 C.
- Parts are carefully de-rated in terms of operating voltage, current, power, temperature, etc., to keep their failure rates low
  - See paper for references to publications that provide component de-rating guidelines.

# Hardware Reliability

- Designers understand how parts fail (failure modes and failure rates)
  - helps provide safeguards against critical effects of the failures.
- Failure mode/mechanism distribution for many parts is found in FMD-97: Failure Mode Distribution Data available from System Reliability Center.

# Hardware Reliability

- Products are designed for the actual use conditions.
- Products are designed to operate in the worst case environment they are intended for. Refer to AREMA MP 11.5.1.
- Products are designed for ease of maintenance and testing
  - See paper for guidelines used.

# Software Reliability

- Supplier community pays a great deal of attention to the differences between hardware and software in terms of their reliability and maintainability.
- This helps ensure the use of right techniques and measures for software design and testing so that overall product reliability and maintainability goals are achieved.

# Hardware vs. Software Reliability

- H/W – failures caused by deficiencies in design, production, and maintenance
- S/W – failure (to perform correctly) primarily due to design faults
  
- H/W – failures due to wear or other energy-related phenomena
- S/W – No wear-out phenomena

# Hardware vs. Software Reliability

- H/W – preventative maintenance can be used to improve reliability
- S/W – no equivalent means to improve software reliability
  
- H/W – reliability is time dependent
- S/W – reliability is not time dependent

# Hardware vs. Software Reliability

- H/W – affected by environmental conditions
- S/W – external environmental conditions do not affect software reliability
  
- H/W – reliability can be predicted in theory from physical basis
- S/W – reliability cannot be predicted from a knowledge of design, usage and environmental stress factors

# Hardware vs. Software Reliability

- H/W – reliability can usually be improved by redundancy
- S/W – reliability can not be improved by redundancy (can be improved by diversity)
  
- H/W – failure rates of components are somewhat predictable
- S/W – failure rates are not predictable

# Hardware vs. Software Reliability

- H/W – interfaces are visual
- S/W – interfaces are conceptual
  
- H/W – uses standard components
- S/W – does not use standard components

# Hardware vs. Software Reliability

- H/W – reuse of proven components can improve reliability
- S/W – reuse of proven software components may not improve reliability due to high interdependencies between modules

# Software Reliability

- Software faults, errors and failures are caused by:
  - Errors of omission – not doing something that should have been done (i.e., incomplete requirements specification)
  - Errors of commission – doing something wrong (i.e., incorrect translation of requirements into software)

# Software Reliability

- Software faults, errors and failures are caused by (cont.):
  - Operational errors – improper (intended or unintended) use of equipment – (i.e., illegal command sequence)

# Software Reliability

- Software faults, errors and failures are mitigated by implementing and following rigorous Software Reliability and Quality Assurance Programs.

# Software Reliability Program Benefits

- Prevent occurrence of faults and errors before software is available for test or use
- Use information developed during software development to eliminate related unobserved faults and errors
- Mitigate the effects of software errors
- Collect project data to improve the processes used to develop software

# Software Quality Assurance Program Benefits

- Conformance to standards, practices and procedures is verified through independent audits and reviews
- Evaluation of conformance to requirements throughout the development life-cycle
- Evaluation of the effectiveness of management and engineering processes

# Software Reliability

- Well-structured, organized and coherent software design methods are used by suppliers:
  - Structured Programming
  - Functional Decomposition
  - Data Structure Design
  - Program Modularity
- These methods help design software such that:
  - Important software components and their inter-relationships are easily identified
  - Software modules are limited in complexity, have minimum interactions with other modules and are easily testable

# Reliability Testing and Improvement

- Suppliers spend a great deal of effort in testing products to ensure their reliability.
- Products are tested during development to ensure compliance with environmental requirements and to identify/eliminate weak points or predominant failure modes.

# Reliability Testing and Improvement

- Tests are conducted to verify compliance with AREMA MP 11.5.1 limits for:
  - Temperature and humidity
  - Vibration and shock
  - Dielectric strength
- Abrasive environmental tests per Mil-STD – 810E
- EMI tests per established national and international standards:
  - Procedures are currently being streamlined by AREMA C38
  - Other references are provided in the paper

# Reliability Predictions

- Failure rates of individual components (per MIL-STD-217F) are used to calculate the predicted failure rate of the product.
- During design, predictions may be used to alter the design or cause component changes to improve reliability.
- Failure rates based on MIL-STD-217F are pessimistic. Actual field failure rates have been shown to be significantly lower.

# Reliability Predictions

- Product actual failure histories are recorded.
- Based on actual recorded failures a revised failure rate can be calculated.
- The accuracy or confidence in these predictions is a function of the number of unit hours of operation achieved, the accuracy of the failure reporting and the method used to calculate the failure rate.

# Maintainability and Availability

- Paper provides formulas for calculating mean time to restore (MTTR), mean time to failure (MTTF), mean time between failures (MTBF) and Availability.
- MTTR is a function of the product's modularity, testability and reparability.
- MTTR does not include travel time and assumes that spare parts are available.

# Maintainability and Availability

- Availability can be improved to very high levels by using active or standby redundancy.
- Active redundancy – two or more channels sharing inputs and delivering common outputs with each channel containing the required health monitoring to allow timely repair and restoration.

# Maintainability and Availability

- Standby redundancy – a working unit with a cold, warm or hot spare. Requires standby unit to be ‘switched’ into operation when the working unit fails.

# Improving reliable designs

- Railroad user community:
  - Keep accurate records of field failures
  - Keep accurate records of the conditions under which failures occurred
  - Provide timely feedback to suppliers
  - Exchange ideas on improving product R&M features, user manuals, training, documentation, etc.

# Conclusions

- Designing reliable & maintainable products is a requirement.
  - Supply community actively works to achieve reliable and maintainable designs
  - The user community can help improve product designs
  - Working together we can improve reliability and maintainability of the signaling products and keep their overall lifecycle costs low.

QUESTIONS?

AREMA C & S May 23, 2006