



## Microprocessed signalling systems: safety and reliability validation

A.C. Merlo, A. Gerecht & G. Pedroso

*CMW Equipamentos SA, R. Rocio 351, 04552-000, São Paulo, Brasil*

### Abstract

As microprocessor technology is becoming more and more advantageous since its use represents a good cost/benefit ratio compared with conventional technology and due to the prudence in regard to new techniques being applied in railway signalling, it has become necessary to develop means for proper systems validation. Techniques such as reliability and safety evaluations, fault tolerance, majority voting, data protection, duplicated software modules and operation integrity checking have continually been refined to meet rigorous requirements for vital and non-vital applications.

CMW Equipamentos S.A. has been developing, several programs of microprocessed signaling equipment applied for transit and railroad systems. Experience regarding equipment validation is being applied to different structures, like: Triple modular Redundancy for Interlocking, Speed Code Generation and Train Detection modules; Dual Checked Redundant and Single Channel Microprocessor combined with diagnostic modules, used for on board Automatic Train Control.

Considering required operational and performance characteristics, each architecture is applied where most convenient. Suitable safety and reliability levels are achieved with 1 out of 1, 2 out of 2 or 2 out of 3 architectures.

This paper describes the methodology that CMW uses for projects with requirements of safety and highly reliable systems and products. It also



## 274 Railway Operations

gives details of the safety assessment procedures employed to evaluate qualitatively and quantitatively reliability and safety, with application examples.

### **1 Introduction**

Dealing with solid state microprocessed railway signalling technology since 1977, CMW Equipamentos S.A. has since then been developing safety, reliability and maintainability procedures for its systems and products.

The introduction of microprocessors into Fail Safe applications as on board ATC and Interlockings was a difficult task, because a whole set of procedures had to be created to built up a comprehensive methodology dealing with safety achievement and proof, having equivalent conventional systems has a reference.

With its inherent complexity involving hardware and software aspects, microprocessors made signalling manufacturers and authorities to think about the development of proper project validation methodologies. At the beginning, the design phase was first addressed. For this phase, systems, hardware and software validation analysis techniques were well developed, taking care of qualitative and quantitative aspects of safety and reliability.

Improving its procedures for safety and reliability assurance, CMW today uses a methodology that addresses all the project phases, which means considering documented control of specification, design (systems, hardware, software), prototype manufacturing and testing, production, factory tests, installation, field tests, commissioning, training, post-operation monitoring and maintenance. Safety and reliability is then guaranteed throughout the complete control of all the project stages. A good partnership with the authorities is an important issue that is considered as part of the processes, in order to guarantee the proper system operation during its whole life cycle.

### **2 Methodology for Safety and Reliability Acceptance**

Safety and Reliability acceptance are treated within a methodology which takes care of six main project phases: System Design, Hardware and Software Design, Manufacturing, Installation and Testing, Commissioning and Revenue Service (Fig. 2).



The methodology is supported, regarding formal documents of equipment descriptions and general inspection and test procedures, by a Quality System, based on the ISO 9001 standard. CMW is an ISO 9001 certified company in Brazil, since 1993.

### System Design

System design starts from the system specification requirements, which are provided by the railway authority. A Functional Specification and a Project Program Plan is then generated; these documents show the system, hardware and software general architectures; the project documentation architecture; personnel with responsibilities and the plans for design, manufacturing, installation and test, commissioning and revenue service.

During the System Design phase, safety assessment and reliability prediction is a common practice, such that the next phase, which is the proper design, will start with some main rules already directed. Some of these main rules are, for instance: blocks should have intrinsically fail safe hardware; processors with single or redundant architectures; components to meet special environmental conditions such as temperature vibration, humidity, atmosphere requirements; EMI and ESD protections.

A Design Review finalizes this phase. At this point, the project is discussed in house and with the Client. The System Specification Requirements should be fulfilled, otherwise the next phase will not proceed.

### Hardware and Software Design

The Hardware Development Plan has standardized procedures defining: Requirements - what to do; Architecture - definition of the hardware modules and their interfaces; Detailed Design and Implementation; Reliability prediction; Prototype testing; Integration.

The Software Development Plan has also standardized procedures defining: Requirements - what to do; Architecture - definition of the software modules, their interfaces and data base definition; Detailed Design and Implementation - successive break down to subfunctions in a top-down approach, up to an acceptable level for codification; Codification itself; Testing; Integration.

Along the Hardware and Software Design phase, a Safety Assessment and Reliability Prediction



## 276 Railway Operations

Analysis is performed by an independent team from the designers.

Safety Assessment and Reliability Prediction is done through a handmade analysis of the project documentation, checking the specifications against the complete design and manufacturing processes. This verification is done observing qualitative and quantitative aspects associated to safety and reliability. The analysis follows a Successive Refinement Process Model (Fig. 1), handling different safety structures such as: system architecture; computer based, redundant architecture and intrinsically failsafe based hardware; software; special tools used for design and or system application. MTBF, MTBUF and MTBUT calculations, FMEA and safety analysis are performed, feeding back to the design team until the operational requirements are fulfilled. For quantitative analysis, Military Handbook 217, adopted for reliability calculations, is applied for all the blocks in their final design, using the Stress Analysis Procedure. Markov models are derived for special structures, such as redundant channels and triplicated architectures. Communication processes for vital data interchange are studied through the Mean Time Between Unsafe Transactions (MTBUT) calculation.

Another formal Design Review is done at this stage, when the design team and the analysis team meet for discussions, adjusting and finalizing the design, which will then be ready for manufacturing.

### Manufacturing

The manufacturing plan defines the procedures to assemble and test all mechanical and electrical modules.

Inspections and procedures follow all the processes during manufacturing, maintaining the product within the design specification. Problems that appear along the processes, like obsolete or equivalent components, cable routing inside cabinets or modules, etc, are formalized and discussed with the design team.

Functional tests are performed for individual parts up to an integrated system test, before releasing equipment for the field.

### Installation and Field Tests

Installation is done according to an Installation Plan that has the inspection, test procedures and the installation design to be applied. The



installation design is usually made following general rules that are defined by the design team during the system, hardware and software design.

Field tests are done for components, modules, subsystems growing up until the complete system to be functionally tested.

### Commissioning

System Acceptance occurs upon the approval of all the project documents related to safety assessment, functional verification and validation and reliability evaluations. This approval is done in house and then with the Client.

### Revenue Service

Field Reliability Verification starts after the system enters normal operation, and is performed over the field data reporting the system functionality. Failure reporting, failure analysis, corrective actions and system reviews are part of a closed-loop process, feeding-back the design team, whenever applied.

## **3 Examples of Application**

This Methodology is being applied by CMW to the following projects which have microprocessor-based fail safe components:

Solid State Interlocking, 2 out of 3 architectures

Metro Authorities: 20 systems

Commuter Authorities: 3 systems

Solid State Interlocking, 1 out of 2 architectures

Long Distance, ATCS: 1 system (under construction)

Solid State AF Track Circuit with embedded Speed Code

Metro Authorities: 9 systems

On board ATC, 2 out of 2 architecture

Metro Authorities: 140 systems

Commuter Authorities: 50 systems

On Board ATC, single processor

Long Distance: 20 systems

Long Distance, ATCS: 25 systems (under construction)



#### **4 Final Comments**

The commitment with high levels of safety and reliability inherent to railway products has pushed the authorities and the manufacturers to develop new rules for designing and manufacturing microprocessed based equipment, since this technology is not as easy to be understood and validated as the well known relay technology is today.

The combination of well defined methods, procedures and standards with a gradual programmed migration of functions from traditional technology into modern technology is strategy that CMW has considered. Part of the success of the Solid State Interlocking application, for instance, was the strategy to first "emulate" conventional equipment with microprocessed hardware and software. Conventional implementation architecture was as much as possible maintained, simplifying in this way, the equipment validation process as well as familiarization with the new technology.

Over recent years, CMW has been improving microprocessed fail safe technology, both in terms of the product itself, and also in terms of the safety and reliability control processes. Some highlights of such methodology are described in this paper. There is still lots of work to do, getting the microprocessor based technology ever more "user friendly" to the signal engineers.

#### **5 References**

1. G. Pedroso, A.P. Rangel, F.J. O. Dias, "CMT: A Fault Tolerant and Fail Safe Microprocessed Interlocking System, COMPRAIL 92.
2. F. J. O. Dias, B.J. Souza, "Safety Assessment Methodology for Railway Systems", COMPRAIL 92.
3. Siewiorek, D.P. and Swarz R.S. The Theory and Practice of Reliable System Design, Digital Press, Bedford, Mass, 1982.
4. Rennels, D.A. "Fault-Tolerant Computing-Concepts and Examples", IEEE Transactions on Computers, Vol C-33, nº 12, pp.1116-1129, December 1984.
5. Petersen, W.W. and Welson Jr. E.J. Error Correcting Codes, Second Edition, MIT Press, Cambridge, Mass., 1972.



6. Musa, J.D., Iannino, A. and Okumoto, K. Software Reliability - Measurements, Prediction, Application, McGraw-Hill, 1987.
7. Dias, F.J.O. and Gerecht, A. "Transmissão Vital de Dados," 16Th Safety Workshop of ABNT, 1990.
8. Dias, F.J.O. "Multiple-Fault Analysis in Combinational Logic Circuits", PhD Thesis, Stanford University, 1975.
9. MIL - HDBK-217, "Reliability Prediction of Electronic Equipments" U.S. Dep. of Defense, 1989.
10. MIL - STD-882, "System Safety Program Requirements", U.S. Dep. of Defense.

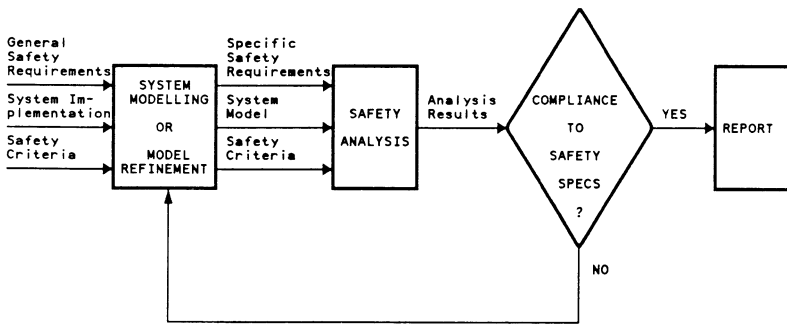


FIGURE 1 - SUCCESSIVE REFINEMENT PROCESS  
MODEL



## 280 Railway Operations

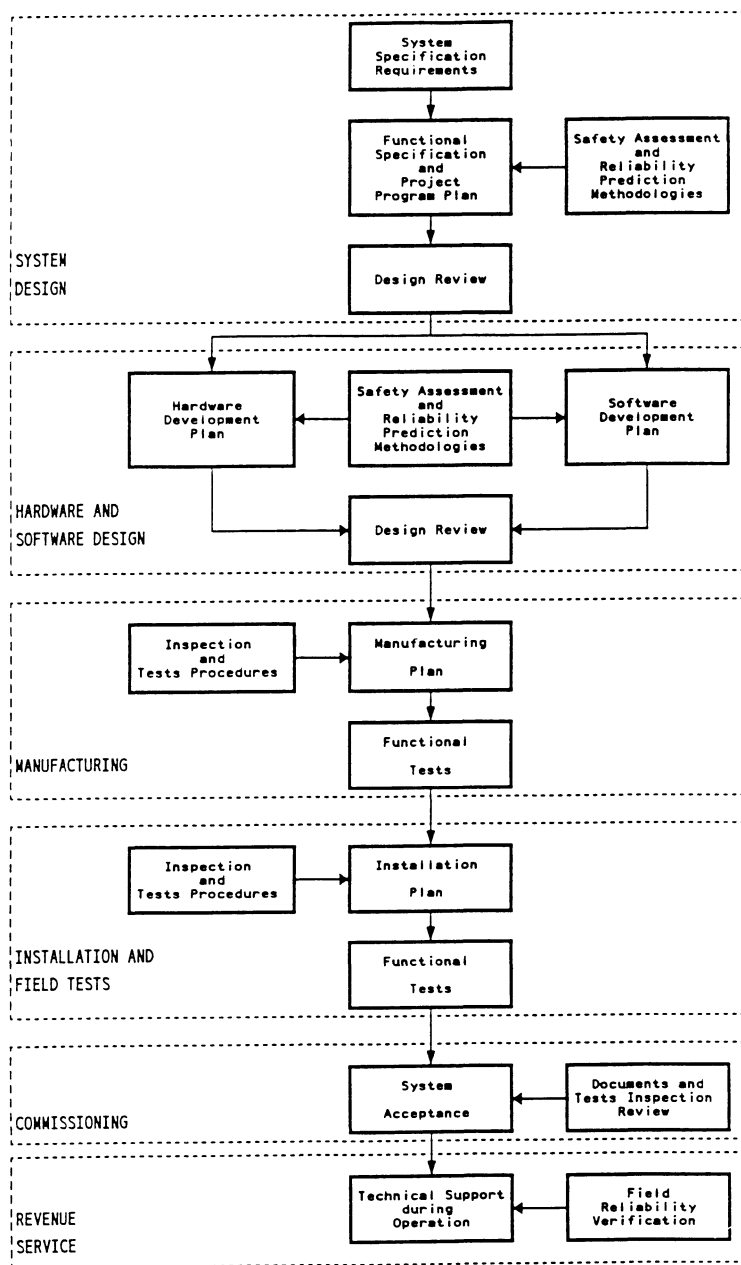


FIGURE 2 - SAFETY AND RELIABILITY ACCEPTANCE PROCESSES FLOW