RELAY LOGIC TECHNOLOGY APPLICATION FOR ROLLING STOCK SAFETY/MISSION CRITICAL CIRCUITS

Best Practises and New Technologies

Warwick Simpson
B.Eng (Elec)(HON)
RailCorp – formerly of Downer EDI Rail

Michael Briggs
B.Eng (Elec)(HON)
Australian Rail Technology

SUMMARY

Despite the worldwide trend to discard traditional technologies in favour of solutions that use smaller, smarter, reconfigurable technologies and services, there are situations where the “old” still has plenty to offer. Relay technology still has the ability to deliver safe, robust and reliable solutions for situations where safety critical and/or mission critical requirements are not negotiable.

Safety and mission critical functions require solutions that feature high integrity and high reliability/availability. They also need, when they fail, to adopt or configure into an operating state that maintains the system’s integrity and overall safety. Relay circuits have a history of being able to satisfy these basic needs. Other technologies such as microprocessors or similar, have to include other specialist processes to ensure system safety requirements are achieved. Relays have a long history with known modes of operation and are quite well observed and understood.

This paper reviews the application of a relay based solution to create a modern train that is safe and reliable to meet the ever-increasing demands of safety standards and legislation, and the ever-increasing system availability targets demanded.

INTRODUCTION

Due to increasingly stringent and demanding targets for safety and reliability, systems are becoming more complex, which usually require solutions with a high level of complexity. However in certain cases simpler solutions can offer better results. With this in mind, the re-emergence of a seemingly old technology of relay logic with its known pros and cons was deployed to meet the design requirements of a modern rolling stock project.

The specification for the Waratah Train Project required the design to address safety and reliability in accordance with standard EN50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) [1]. This was to provide reliable design solutions for the train ‘safety critical’ and ‘mission critical’ systems needed for safe and reliable operation of a modern train fleet as demanded by today’s standards.

The well known technology of relay logic, which has had a history of being safe and reliable since electric control circuits were added into train designs after the steam age, was brought back to life with a twist of modernisation to make the design, delivery and implementation of the safety and mission critical circuits within the Waratah Trains capable of meeting today’s demanding requirements. This paper will discuss how this emerging technology, which is known as the Form Fit Relay Solution (FFRS), has addressed the project’s needs in areas such as design life, space constraints, configuration management, future expansion and being able to easily troubleshoot problems.
Relay Logic Technology Application for Rolling Stock
Safety/Mission Critical Circuits

NOTATION

ALARP As Low As Reasonably Practicable
ATP Automatic Train Protection
CM Configuration Management
CSA Cross sectional Area
DTR Digital Train Radio
FFRS Form Fit Relay Solution
LRU Lowest Replaceable Unit
MC Motor Car
MCBF Mean Cycles Between Failure
PCA Printed Circuit Assembly
PCB Printed Circuit Board
RAMS Reliability, Availability, Maintainability and Safety
SIL Safety Integrity Level
SNCF Société Nationale des Chemins de fer français; or "National Corporation of French Railways"
TC Trailer Car
TDC-L8 Trailer Driver Car – Locker 8
TLS Through Life Support
TTL Transistor Transistor Level
4PDT 4 Pole Double Throw

RELAY COMPONENTS FOR SAFETY AND MISSION CRITICAL CIRCUITS

Relay logic, with real relay contacts and coils, has been deployed over a vast array of projects and has been successful in providing high integrity circuits for safety critical circuits and mission critical applications. In the past, the relays have been conventionally mounted on DIN rail or panel mount situations, with hard wiring connecting the various circuit elements together to produce the relay logic desired. The circuits to be deployed could only be relatively simple, as the relay elements occupied significant space within the equipment enclosures as shown in Figure 1 and Figure 2.

Relay elements with rather specialised functions, featuring non-overlapping contacts, were available. With these elements, if one contact pair was to be welded together, all other contact pairs would also show a closed circuit, thus allowing single point failures to be detected. Delay ON, Delay OFF and voltage sensing contact operations were also available for specific sequencing operations. The fore-mentioned are only a few examples of what could be achieved with relay logic. The Form Fit Relay solution is a technology that enables application of all of these features and configurations as the main elements being used are individual relay devices that are available at a fraction of the size of conventional legacy relays. Following the design review process the Form Fit Relay Solution was selected for implementing various safety and mission critical circuits of the Waratah Train Project.

Figure 1 – Legacy system of approximately 90 Relays (Cabinet size 1800 x 482 x 500mm)

Figure 2 - Rear view of associated relay wiring

THE FORM-FIT RELAY SOLUTION

The Form Fit Relay Solution is the integration of printed circuit board (PCB) mounted rail specific electro-mechanical relays and timer devices. These printed circuit assemblies (PCA) are joined to form modules based on Eurocard formats,
which are loaded into a sub rack assembly as shown in Figure 3. From the backplane to the train connectors, intermediary wiring with easily configurable links create the internal logic including interlocks and parallel (redundant) circuits. This system allows for a high density of relays in the given space, with solid electrical connections between circuit devices.

The Form Fit Relay Solution is mounted in a 19” rack enclosure which can be mounted in a clean environment or under frame in a sealed enclosure. The limiting factor is the supporting components, connectors and hardware.

These relays are anything but old fashioned. They are highly reliable, hermetically sealed with balanced force armatures and non-overlapping contact design. A typical relay measures just 26 x 26 x 26mm, as shown in Figure 4.

The relays have the following characteristics;

- High reliability – 2 million electrical operations based on conditions depicted in Figure 5.
- Hermetically sealed – sealed to IP68.
- Nitrogen filled to reduce spark when breaking contact.
- Non-overlapping contacts – prevents any contacts within the relay from performing a simultaneous Normally Open/Normally Closed combination.
- Small size of the relay combined with the balance force armature (magnetic flux) yields long mechanical life and excellent resistance to vibration.
- The balanced force armature design of these relays allows for flexibility in the mounting orientation.
- No spring element for armature retention. See Figure 6 and Figure 7.
- Not susceptible to typical EMC emissions.
- External surge energy is absorbed by suppression devices mounted on the relay PCB.

These relays are anything but old fashioned. They are highly reliable, hermetically sealed with balanced force armatures and non-overlapping contact design. A typical relay measures just 26 x 26 x 26mm, as shown in Figure 4.

COMPONENT SELECTION – THE RELAY

After having made the choice to use a relay based solution, the market was explored to identify what was available. Leach International Europe of France has been at the forefront of relay manufacture for over 60 years. The organisation primarily caters for the aerospace industry, and their customer base includes NASA, Boeing and Airbus. Leach International Europe commenced supplying relays on PCBs for SNCF (French Government Railways), over 10 years ago. Initial use was limited to mid-life upgrades and modification. Over time these designs grew and became more widely accepted throughout Europe, allowing the Waratah Train Project design engineers to inspect and obtain feedback from train operators in the United Kingdom.

Due to the combination of these relays and Leach International Europe’s involvement in rail, the French have developed standards such as reference item [2] specifying relay application for railways that do not exist elsewhere, and are regarded as world leaders in the field. With this in mind, it was not a difficult decision for the Waratah Train Project to select these relays and use them as the foundation for an advanced safety/mission critical system.
• Relay coil back EMF and self generated spikes are controlled by flyback diodes connected across the coil elements.
• Short term overload ratings.

**THE RELAY CARD MODULES**

Seven base PCBs form the building blocks and are used to create 22 unique modules (see Figure 8 and Figure 9). These modules are used in 76 module slots in the six different sub rack assemblies required. A total of 14 sub rack assemblies are fitted to an eight-car Waratah train set. For simplicity and illustration Figure 10 shows the sub rack types and positions on 4 out of the 8 cars that comprise a Waratah Train set.

The 22 modules thus become the Lowest Replaceable Unit (LRU) and consist of 2 pole, 4 pole, 6 pole, 11 pole and 18 pole relays combined with special functions of Double Make/Double Break (DMDB - higher current) Delay ON, Delay OFF, voltage sensing, latching and flashing relays. These modules can be easily changed out during maintenance activities.

The standard timers are programmable (via PCB solder links) from 0.25 to 63 seconds (in 0.25 second steps) and 0.25 to 63 minutes (in 0.25 minute steps).
required. For the large sub rack frame (see Figure 3) there was a need to accommodate a set back mounting flange and a higher than expected weight for the loaded sub rack design. The selected sub rack frame chosen was only compliant to 10kg (as tested by the supplier). The largest sub rack weighed 25kg with all relay card modules fitted. New mounting flanges and bracing were designed to accommodate the higher weight and the new location of the mounting flange. Both of these additions saw the sub rack pass shock and vibration test.

The smaller sub rack (see Figure 11) was not to be located in a traditional 19 inch rack. It was to be located in a confined space, hence the sloping top. Also as less functionality was required (less relay card modules) the sub rack frame was narrower than the standard 19 inch frame.

As Figure 11 shows, a ‘top hat’ extension was required in order to accommodate the train connectors and intermediary wiring. The ‘top hat’ extension was designed to integrate with the off the shelf sub rack metal work. The smaller FFRS sub rack was tested and passed without issue.

**SAFETY AND RELIABILITY**

The safety circuit designs required to meet the specification requirements for the Waratah Trains were able to be deployed with proven, readily available relay elements despite the rigour of the design work demanded for compliance with [1]. The circuit designs were:

- Reviewed for their functional and safety performance.
- Implemented to have fail-safe circuit operation and redundant mechanisms.

Analysis, studies and design work to address the requirements of [1] produced a number of documented outcomes for the areas of:

- Operational concepts.
- Safety target apportionment.
- Availability prediction reports.
- Reliability prediction reports.
- Maintainability prediction reports.

Resulting from this, the main safety and mission critical circuits implemented with the FFRS includes:

- Transmission of train line signals for traction and brake demand of power, brake, forward, reverse.
- Traction interlock/inhibit when a side door is not closed and locked.
- Crew bell communications.
- Door open and close commands.
- Operator enable pedal.
- Buffering and re-transmitting vigilance commands/actions.

Since the train is comprised of multiple units, with many sub-systems such as traction and braking distributed over all cars in the train, the control circuits of the train are also distributed so that no one safety or mission critical function is performed by a single relay sub rack.

The following is a brief failure rate analysis discussion on the FFRS implementation of a specific safety function to contain the passengers within the cars while in motion with doors closed. This specific safety function is controlled by the following components:

- Door Control Unit (DCU) at each train side doorway.
- Train wiring and terminations
- Door ‘open and ‘close’ buttons
- Relays within the FFRS sub rack.

The DCU chosen for this function is an industry available product and comes with an established SIL2 rating. In this application the recognised probability of dangerous failure per demand allowed from [1] is between $10^{-3}$ and $10^{-2}$. Therefore in order to maintain the integrity
provided by the DCU, the task of conveying the crew request to close and maintain closed the side doors on the train the system components had to meet or exceed SIL2.

A crew operated pushbutton and a combination of FFRS devices (with a basic failure rate of $3.38 \times 10^{-6}$ for each relay device) is shown in the simplified example (Figure 12). Four interlock relay contacts are needed in order for a door open command to be realised. The combined failure rate is $13.5 \times 10^{-6}$.

The resulting failure rate for the FFRS combinational logic is well below the limit and would not downgrade the established SIL2 rating for this safety function.

![Figure 12 - Door open interlocks](image)

Other safety and mission critical functions were designed with FFRS components based on the outcomes from the initial [1] analysis described above.

Relay circuits also allow for simple analysis of device functional reliability to be performed. The devices can be operationally analysed and a value calculated for the Mean Cycles Between Failures (MCBF). MCBF is a more appropriate measure as a relay’s service life is dependent on the number of operation cycles and not the number of years.

With this information and with the application of appropriate safety factors, planned maintenance can be performed with the knowledge that the device will not suffer failure before a known timeframe. This will lead to the development of an appropriate replacement programme for devices that are considered to be at the end of their life, thereby minimising random system faults in general operation. With the relay devices also directly switching the actual currents used in the external circuits, the operation of the relay can be predicted for the true environment in which it is installed. It is not masked by the reliability of a component or module performing an interfacing function which is generally required to translate the TTL style logic gate (or similar) signal level into the voltage signals required by the external equipment.

**THE FFRS DESIGN, MANUFACTURE, TEST AND THROUGH LIFE PHASES**

During the initial phase of any design project, the design engineer is required to identify and engage the relevant stakeholders to ensure that the designed solution will address their needs and expectations. For the Waratah Train Project [1] was used as a reference baseline to identify and consider relevant stakeholder needs and expectations in conjunction with the safety and mission critical objectives. The deployment and inclusion of relay modules within the final solution for the safety and mission critical circuits will allow all the relevant needs identified to be addressed.

As an example, the train circuit for the train door open and close functionality had to address the following needs:

- **Operator (Guard and Driver) needs** – Simple, reliable and robust.
- **Designer needs** – High integrity, fail safe, integrated and independence from other systems.
- **Through Life Support (TLS) needs** – Low part count, no obsolescence issues, maintainable system without special tooling and long life.
- **Owner needs** – Reliable, repeatable operation.

The design engineers were also required to accommodate information fed back from the following phases as inputs to continually refine the solution design.

- **Manufacture.**
- **Test and Commissioning.**
- **Through Life Support (TLS).**

The solution development process included a prototyping phase where any findings from rectifying design defects identified during the course of testing and maintaining the prototypes needed to be fed back as inputs into the solution design.

Initially prototypes of the design were produced in small batch runs. Once the design was proven to be operationally stable, project quantities of the modules were produced. During the testing phase,
the modular nature of the relay modules, and the flexibility provided by the intermediary wiring circuit components allowed design changes to be made and documented.

The manufacturing team were also an integral part of the prototyping process and received feedback from testing to improve the build process. When full production was needed, the mass production process involved the manufacture of high volumes of the building block modules, with the final circuits being customised for their specific function and location on the train in the final assembly phase of the completed rack. Efficient mass production of ‘simple’ components was promoted.

Tracking design and equipment build configuration was a relatively simple task as the Configuration Management system (CM) only has to manage and track the version state of the equipment. There was no software element to track, nor any and track the version state of the equipment. There was no software element to track, nor any complex combinations of a software version not working on a particular hardware combination (before or after a certain date), and vice versa. The existing tools of the CM system were utilised to manage the version state of the FFRS equipment as changes from testing and design change were implemented.

With the design being an assembly of building blocks, any changes to the system during the through life phase can be achieved by re-arranging the blocks and making simple internal wiring changes to the sub racks. Troubleshooting a fault with the system can be easily undertaken because maintenance personnel deal with real system voltages that are present in the remainder of the train. The simple circuits can be understood and analysed without sophisticated test equipment and logic analysers. Furthermore, the modules (the LRU) or the whole sub rack can be readily changed out when the fault is identified, and the stock holding of maintenance spares can be adjusted based on the number of unique modules needed for the system.

The Waratah Trains will undergo future modifications and enhancements. Two systems that have had allowances made at the establishment of the design baseline are Automatic Train Protection (ATP) and Digital Train Radio (DTR). Currently, within the FFRS, a shunt module has been provided, which when changed with a new ATP module will facilitate the change to the logic of the safety and mission critical circuits that need to be interfaced to the ATP equipment. This will be a simple change that can be implemented at any stage of the life of the train and will not trigger any obsolescence issues with the FFRS equipment.

The FFRS is in line with industry trends of developing new solutions with increased system functionality accompanied by small form factors. Modern trains need to increase the passenger carrying capacity with each new design, and introduce new features such as on-board surveillance recording and analysis, integrated train equipment monitoring equipment to assist in the diagnosis of train faults, passenger information systems and added access paths for the disabled members of the community. All of these needs can be realised by the FFRS.

MANUFACTURING BEST PRACTICES

A project of the size of the Waratah Trains is exposed to many manufacturing issues. The two most important that will be discussed in this paper are;

- Human versus automated testing.
- Quality crimping.

Reference items [3, 4] discuss the investigation of errors in systems and processes, and how to understand and overcome them. One of the main points highlighted is that “humans are fallible and errors are to be expected” [4]. Due to the nature of the sub racks requiring hand assembly for the intermediary wiring, it was important to ensure this wiring was correct. This is essential for mission and safety critical circuits.

The quality and consistency of the manual intermediary wiring work was addressed in three stages:

- By testing the continuity of all wires after assembly. This was a low voltage computer test capable of testing the near 1800 points required on each sub rack. This will determine if any crossed or open circuits exist.

- Performing an industry standard high voltage potential test to confirm that none of the wires in the sub rack had damaged insulation or circuit imperfections.

- The completed sub rack was then connected to a custom built Automatic Test System to functionally test the FFRS at the nominal train voltage to verify all circuits, timer settings and voltage level sensing equipment.

With a 35-year design life and volume of almost 10,000 crimps per FFRS set, it was important to ensure a quality crimp. The three methods available to analyse a crimp are Dimensional Checks, Pull Test and Cross Sectional Analysis.

Dimensional Checks measure the height of the crimp, and the Pull Test destructively measures the holding force of the crimp. Both of these techniques provide an indication only, that the crimp is satisfactory.
The Cross Sectional Analysis (CSA) or ‘cut and polish’ is the most thorough technique available to confirm a quality crimp. This method allows examination of each wire within the crimp under a microscope to verify that the wires are evenly deformed and that no voids are present. The presence of voids can lead to corrosion compromising the crimp over the long term, see Figure 13. CSA has not been a popular approach due to cost. However new equipment from Europe allows CSA examination on a regular basis to ensure quality products. These practices are needed for the production of equipment being used in safety critical and mission critical circuits.

During manufacture each sub rack type has a sample wire subjected to a pull test, and a dimension check at the start and end of the sub rack type wire loom assembly. Furthermore, for each set manufactured, a CSA is conducted to verify that the crimping tools are still compressing all strands of the wire correctly as shown in Figure 14.

**WHAT IS WRONG WITH A SOFTWARE SOLUTION? WELL NOTHING, BUT...**

The advent of the Programmable Logic Controller (PLC) was promoted as being the ultimate flexible tool to use for control logic in systems. It could be modified and expanded, and the characteristic of the system changed completely and immediately with a quick change of its internal software, and for certain cases some external hardware changes. This in principal was a great step forward for most control systems where time consuming modifications to a hardware based control system was not possible, or if the plant was being re-configured to be used for another purpose. However, it is now expected that the design of software based systems to be used for the operation of safety critical functions, need to be engineered and designed using recognised standards for structured approach to software and system development. This is the methodology documented in [1].

The design of safety circuits for use on train systems has to also follow the same rigorous process documented in the standard. The software for use on a safety related system requires that the safety integrity level (SIL) for the system is established, and then the software and the system follow a design process that ensures the SIL determined for this development is achieved, demonstrated and maintained for the life of the design. For the Waratah Train Project, a software solution would introduce a level of engineering design development that would be uneconomical when compared to a traditional relay logic design.

The use of other logical implementations such as Field Programmable Gate Arrays - which may not suffer from random programme execution once an unpredicted exception occurs within the software programme or whilst trying to execute the intended software – do require a similar level of software/logic development – and as a result was not considered for the Waratah Train Project. This argument applies to any software based solution.

Any software solution also needs interface hardware to translate the logic results from the software module into the real world. This hardware is usually TTL type components that then need to drive solenoids, contactors and actuators. This introduces another layer to be analysed, validated and maintained.

The designers of the safety and mission critical circuits on the Waratah Train chose to use the relay logic implemented with real relays rather than a software solution due to economic factors, space constraints, obsolescence and through life considerations.
CONCLUSION

The Waratah Train Project has been able to overcome the industry considered downsides of relay systems to produce the “Form Fit Relay Solution” which has also facilitated:

- Solutions that meet the requirements of a rail system.
- Concurrent development and design, avoiding lengthy delays for safety certification.
- An increase in the relay per volume ratio.
- Rack and sub rack components utilising PCB and other space saving techniques.
- Systems that can be expanded.
- A system of “swap out” of like modules to identify faulty components and minimise system downtime.
- Off-site repairs of modules or sub racks for better quality, more up-time and less spare holdings.
- The re-direction of labour intensive ‘relay cabinet’ wiring to automated mass production techniques, thus allowing for redeployment of that labour into the remaining labour intensive areas to reduce the likelihood of errors in those areas.

The relay devices that form the basis for FFRS have been widely used in aerospace design, and will receive increasing recognition and application in trains.

The use of advanced versions of a seemingly old and sometimes underrated technology in the development of solutions for safety and/or mission critical circuits in accordance with the requirements in [1] ensures the future of the Form Fit Relay Solution in train design.

The Form Fit Relay Solution makes good use of the benefits of conventional relay technology at a fraction of the usual volume occupied by conventional relays.

The result is a modern train that is safe and reliable which uses an advanced relay solution.

REFERENCES