Programmable logic or electromechanical circuits

a comparison

Monday 21 September 2020

Abstract

Desiging systems and functions in complex systems is shifting more and more into programmable logic controllers, but more than often the benefits do not outweigh the costs in terms of design time and complexity. A fundamentally more simple design is often more reliable and has less design and certification risks.

Introduction

With digitalization of the railway market many electronic control systems are introduced in railway vehicles and wayside systems. Digital control of systems offers many advantages over more traditional control systems. With the Internet of Things assets in railway become more and more connected. But is a digital control system always the best solution to achieve the goals of a reliable and affordable railway system? Do we trust connected digital devices with the most safe and secure tasks?

Levels of digitalization

Since the eighties of the previous century digital computers started to take over the control of machines. PLC's (Programmable Logic Controllers) and later ICU's (Intelligent Control Units) got the task to control the ever increasing complexity of systems. Monitoring tasks have been gradually introduced and at some point online remote monitoring became the standard for new equipment. At the highest grade of digitalization even the control task is remotely connected and field systems are controlled from the cloud.

A major upside of this is the ability to monitor and control the system as a whole without the necessary intervention of people. There is no denial in the fact that this transformed the rail industry and allows for a higher performance levels than ever before. There is however a big downside to the sole use of digital systems. The design complexity has grown well over the boundaries of what a single system designer can comprehend. Several ISO, IEC and EN standards[1] are in place to cover the challenges of complex system design. Even greater efforts are made to recognize failure modes and ways to keep systems safe during failures. Failures are inevitable. In complex systems it is not at all uncommon that at any given time some component in the system is unavailable. Furthermore cybersecurity is an even greater growing concern.

Maintaining high availability with increasingly complex systems

Complexity often comes with an increased parts count. Traditional reliability calculations (MIL-HDBK-217, FIDES) use parts count methods to estimate the failure rate of a system. Although the accuracy of the prediction is debatable, it is evident that with an increased parts count the reliability decreases. To overcome this fact, while maintaining the advantages of digital connected systems, an adjusted approach seems necessary.

Systems often have complex interfacing requirements, but in the end only a few interconnections are really relevant for the functionality and safety. For example a traction system: driver inputs, speed signals, motor temperature information, perhaps even modelled derating curves based on air pressure and ambient temperature and previous excitation, cloud-derived track adhesion performance parameters and such all may eventually control the motor frequency and voltage. But what it all boils down two are the power lines to the motors and the electric power they carry. Although probably less evident, many systems have a similar construction. A wide list of parameters control only but a few crucial signals. In reference of Pareto: 80% of the variables are used to only control 20% of the performance output. Inversely 20% of the components provide 80% of the functionality.

[1] for example the systems engineering standards ISO/IEC/IEEE 15288, EN/ISO/IEC/IEEE 29148, standards for RAMS demonstration EN 50126/50128/50129/61508

Design efforts are mostly invested in the 80% that do only marginally contribute to the performance output. Sometimes well over 95% of design costs are in software, digital control systems and the validation of the combination within the system. A parameter that attributes 2% of the system performance may take 10% of the design effort. On the other hand, the basic and proven concepts of the low level technology in a system require only little design effort, while having a large positive effect on the performance of the function. For example electro-magnetic interference (EMI). Many expenses to certify a system go into designing low susceptibility to EMI, and limiting emission simultaneously. Hours and hours of testing, simulation, pre-compliant measurements and compliance certification are required to get the "EMC approved" stamp – per region and relevant standard if you export equipment over the continents and for different industries –. And apart from hours of work, also the parts count increases, which results in yet more costs for parts and assembly. But how much simpler would an intrinsic EMI-compliant design be?

Seen in this light it seems illogical to shift basic functions that are well performed by low level technology to high level digital components. Basic safety features like an emergency cut off of traction motor supplies are hard to integrate in software, but easy to create in, for example, relays. Even control features are often simpler and more reliably done in relays than in an ICU. The digitalization of the control system may still be a goal to strive for, but overcoming the cumbersome translation from the fine-grained digital world to the more robust world of power control may be best left to the simpler devices like electro-mechanical relays.

ASPECT	RELAYS	ICU's, PLC's, MICROCONTROLLERS
Robustness	Highly	Little to moderate
EMI-susceptibility	Inherent superb	To be tested/certified in assembly
EMI-emission	Contained	To be tested/certified in assembly
Design and simulation	Easy, fast	Hardware, software aspects
Verification/Validation	Easy to model failure modes	Hard to evaluatie HW/SW interactions

Conclusion

Current times provide many ways of designing fancy electronic controls with software control. This brings loads of functions, but also extra costs and added complexity in certification. Simpler designs based on relays are often intrinsically EMI-compliant and easier to validate. Design time is spent more to create the function, and less on the certification aspects of the product. This may often lead to shorter times to market and lower costs while gaining higher reliability.

About the author

Mr. René Knuvers (1974) is educated in electric and electronic engineering (BSc degree) and works in railway vehicle design since 1997. In various positions with NS (Dutch state-owned rail operator) and LUCROS Railway Engineering he was responsible for the design, maintenance and modification of electric and electronic systems ranging from doorcontrol to climate systems and automatic train protection to passenger alarm systems. Landmark projects have been the integration of ERTMS/ETCS, ATB, PZB, SHP, KVB and Crocodile for multiple cross border locomotive types on the European continent.

LUCROS Railway Engineering is a Dutch engineering company with a sole focus on engineering for railway applications. Experienced LUCROS engineers make reliable and safe designs for urban, mainline and highspeed passenger and freught rail vehicles every day. All types of technology and integration levels are covered, from ground up electrical system design, to integration of highly complex digital electronic systems.