Reliable and efficient embedded systems design - real-world experience from a large design project

Johan Pensar
Wärtsilä Finland Oy
Järvikatu 2
Vaasa, Finland
Tel.: +358 40 592 9632
E-Mail: johan.pensar@wartsila.com
URL: http://www.wartsila.com

Keywords

Industrial application, Reliability, Systems engineering

Abstract

Traditionally, when a high reliability and safety has been requested for various machines and systems, this has largely been accomplished using mechanical solutions, while the use of electronic systems has been minimized. Modern machines and systems are, however, more and more fully depending on electronic control in some form, and thereby the reliability of the electronic control system is heavily influencing the reliability of the machine itself.
A major part of commercial electronic systems produced today are related to applications where an outmost reliability and aspects like human safety are not an issue. Therefore, conventional development and validation methods used for this type of applications are not necessarily directly applicable for designs where a high reliability and safety is required. In particular, when requirements for efficiency in the design cycle also are expected, this calls for special methods.
This paper describes a case study of the design of a new embedded control system for large diesel engines. In the design of the system, the efficiency of the implementation, testing and validation was studied, and a method supporting a more efficient implementation process was implemented. In the case study, it was noticed that not only substantial savings in form of a more efficient embedded systems development can be reached, but also that the quality of the embedded design will increase significantly.

Introduction

With the increasing requirements on performance and functionality, the use of electronic controllers is increasing in most areas of technology. With “smart” control, it is possible to measure and control machinery better, faster and with less equipment than ever before. The possibilities of smart control are also continuously evolving, allowing more data to be retrieved from the same measurements as before, to get a better performance from the same actuators, and to give a more logical and simpler way of handling the machinery for the operator.
For demanding applications like marine propulsion and industrial power generation, reliability is an obvious requirement. Reliability is commonly associated with fundamentals like safety and with the commercial feasibility of the operation. Reliability does, however, also affect other factors like ease of use, service schedules, skills requirements etc, all with far reaching consequences.
Reliability in a programmable electronic system is, however, not to be taken as granted. Even if programmable electronics is widely used today, few examples on how to combine efficiency and time to market with a high reliability and quality have been shown. More visible are the failures to do so, with numerous examples published. Although numerous examples, books and standards on how to do e.g. “proper” software engineering, hardware validation and system integration are available, the area of efficient embedded systems engineering is in a state of transition, with new methods being introduced.

In the sequel, some of the key factors in the development of reliable embedded systems are discussed from an industrial applications point of view. The key elements focused on standardization, validation and a modern tool-based environment. The system in question is a proprietary embedded engine control system for large reciprocating gas and diesel engines called UNIC – an abbreviation for UNIfied Controls.

The system

To reach a very high reliability in a demanding industrial environment, the system has been designed from the ground up with the sole purpose of providing an excellent reliability even at the most extreme condition. The decision to introduce a custom built control system in an industrial market dominated by mass produced and relatively inexpensive process control systems was deemed a necessity due to performance, but before all reliability reasons, as no commercial off-the-shelf solution was considered reliable enough subject to the demanding operating environment. The reliability was achieved using some, even quite unique, designs and solutions that are not readily available elsewhere [1][2], where the measures to reach the high reliability covered not only the obvious parts of the embedded controls, but the complete installation.
One such example are the sensors. Sensors are often in the design of an engine control system somewhat neglected, as sensors are relatively inexpensive and readily available off the shelf. In practice, however, the reliability of the sensor is extremely important for the system, partly due to the number of sensors on an engine, but also due to the fact that the sensors are commonly mounted at rather challenging places in direct contact with hot surfaces, vibrating components and aggressive chemicals.
Evaluating sensor failures, it is clear that one of the main reasons for failures is actually not the sensor itself, but the connector mounted on the sensor. In UNIC, all sensors have been redesigned for the outmost reliability by removing the connector, and using a fixes attached cable – a flying lead – that connects directly to the electronics. By this design, the reliability of the numerous sensors on the engine has been improved by magnitudes.
Other examples where a proper design heavily influences the reliability are e.g. connectors and cables. Common in e.g. the automotive industry, so called wire harnesses with a lot of connectors, unshielded wires and a lot of fragile plastic parts are not used. Instead, the wiring concept was selected to be based on rugged point-to-point cables, that are very robust and easy to repair and replace in the field.
In order to meet requirements on scalability and flexibility, the obvious system architecture was a distributed, bus-based system.

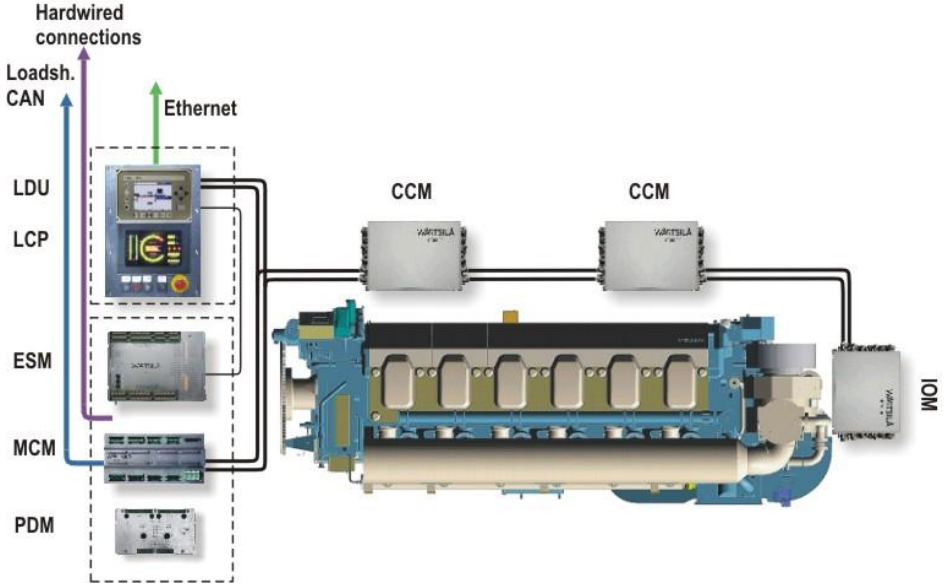

Figure 1 - UNIC system architecture

In a bus-based system, needed functionality can easily be added by adding more control modules, and the system also flexibly adapts to varying engine sizes. To meet the reliability concerns, the system is based on a redundant CAN bus, and will also in an intelligent manner manage with failing hardware components, as functionality flexibly will move from one node to another. It is obvious that the distributed system heavily depends on rather complex software in order to properly control the engine.

Reliable software

The software platform is focused on a reliable end product. Modularization and object oriented programming approaches are fundamentals in any such design. A modular software design allows for pre-tested software modules to be reused in various applications, and significantly speeds up both the coding as well as the testing process.

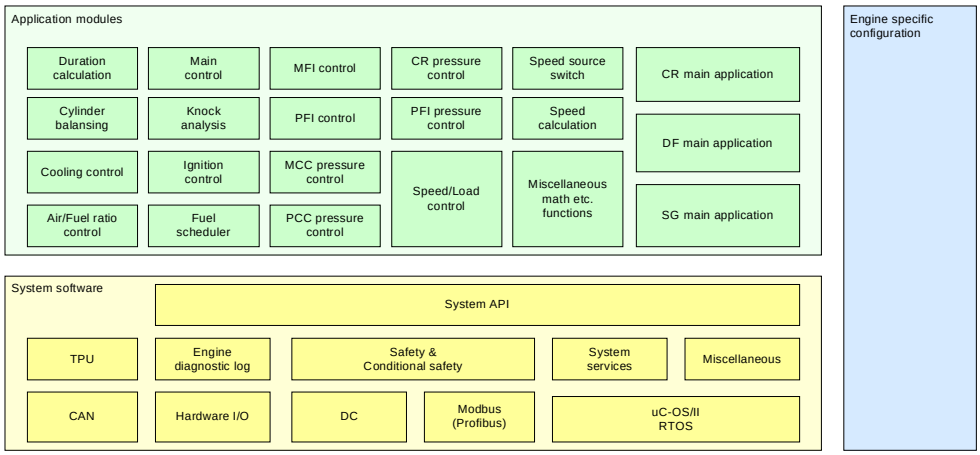

Figure 2 -Software modularity

To create the individual software modules, a flexibility to use the best suitable method was considered optimal. Therefore, in addition to common C programming, the development can also be done using advanced simulation and modeling tools, where the functionality can be modeled and simulated together with an process model until perfected. A move from traditional software implementation methods and implementation cycles can also be anticipated in embedded coding also elsewhere as textual coding languages like C are little by little giving way to graphical programming tools – a move that has been maybe most visible within the automotive industry. Just looking at the move from a textual to a graphical way of implementation is, however, missing the point. The real advantage is more the total integration of the tool-chain, from initial idea to final implementation. Therefore, a commercial tool [4] was evaluated [3] for the possibilities to achieve a total integration in the system platform.
The efficiency is, however, largely coming from the fact that the embedded code can be modeled and simulated together with a model of the controlled process during all phases of the design. This introduces a “virtual engineering step” where the software can be implemented, tested and validated on a workstation, within a process control framework, without ever having to think of any actual coding. When having the process control ready and validated in the modeling environment, the task moving it to a real platform is trivial. In addition, the complete software implementation is depending on something called “configuration” in Figure 2. In order to remove any dependency on coding from the production of the complete code-package for an engine, another tool was integrated with the tool-chain, a configuration tool. From this configuration tool, the complete system is possible to define – again using a graphical interface- without any coding, all the way down to selecting applicable software modules and their scheduling.
The experience from this tool-chain have been good, and the efficiency and quality of the parts covered by the tool-chain have dramatically increased.

Meeting official requirements on software design processes, the final software and hardware integration tests also have to be carried out in a real-life like environment. Manual testing of new software only to the most essential parts has been estimated to several months of work. To speed up this part, automatic testing and validation were also introduced. By automation, the tedious task of manual testing could be speeded up to some days of unattended automatic testing.

Figure 3 - Automated testrig

Hardware reliability

Hardware design for a reciprocating engine might be demanding in many respects. High vibration levels, high temperatures, temperature cycling, electromagnetic disturbances and aggressive chemicals all affect the lifespan of the electronics.
Meeting reliability targets comes down to some basic principles – experience, standardization and validation. Experience is the most valuable part, as in practice an experienced designer may avoid most problems already in the design phase. Standardization also helps, as this avoids introducing new unknowns in the design, but rather basing the design on proven and sound principles.

A key element to reach a good reliability and life expectancy of the system is nevertheless testing and validation – as this is where any weakness is observed and corrected before reaching a full scale manufacturing stage. In some industries, lifetime testing with a representative number of cycles may be possible, but when testing electronic components for e.g. a lifetime target of 50.000 hours, this becomes unrealistically time-consuming as the results would be available after many years of testing, and would also be very expensive to carry out. In reality, this emphasizes the importance of the standardization and experience mentioned above, and leaves only one possibility for the hardware validation – namely various types of accelerated lifetime testing.

Accelerated lifetime testing, known under acronyms like HALT or MEOST, differs from many previous methods. Typically, accelerated test methods are subjecting the device under test to a number of different simultaneous stress factors, like multiple-axis vibrations and shocks, temperatures and temperature cycles, humidity and operational stresses like supply voltage variations and high driver currents. In addition, the test-level for the different stress factors is searched by a certain methodology, and usually set much higher than any normal operation of the device would ever cause. Notably, accelerated lifetime testing methods seldom are able to accurately determine an expected lifetime for a device, but merely detect any design weakness at an early stage.

This type of testing can be considered a current state of the art in terms of reliable hardware design and in particular its validation. The problem with the method is that although rather well received by large scale high-tech industry as aerospace and military designs, the method is still seldom used for more commonplace devices due to a lack of knowledge and a lack of suitable testing equipment. The know-how in interpreting the HALT test results, and in particular any estimation of reliability and lifetime expectancy is extremely demanding. In combination with HALT, methods like failure mechanism modeling using physics of failure models, as well as electronic and thermal simulations, are required as means to validate the design.

The experience of the testing is in general positive. A number of problems have been detected and corrected in an early design phase. Typical weaknesses that can be observed in the tests are of mechanical nature – components breaking loose due to vibrations or due to temperature cycling. As an example, see 4, where a capacitor has broken loose due to vibrations, and the design should be improved by adding glue to bind the component to the circuit board.

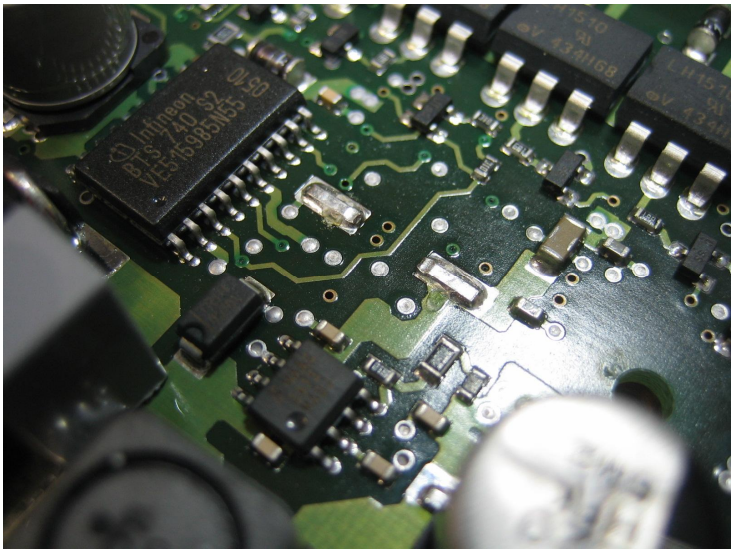

Figure 4 - Circuit board with capacitor broken loose

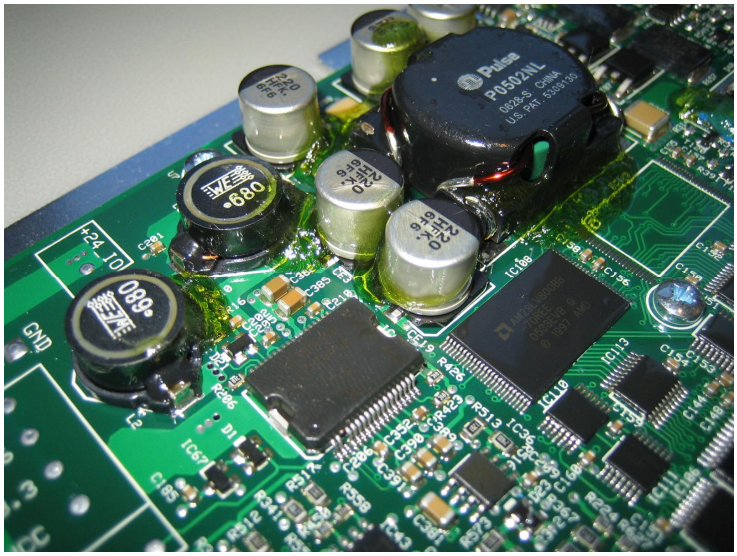

Figure 5 - Glued capacitors as a remedy

When comparing accelerated testing with traditional test methods, like utilizing a one-axis vibration test device and a climate chamber, it has been noted that combined stress testing is capable of

exposing design weaknesses faster, leading to a shorter testtime, but also exposing some problems not occurring during normal tests.

As an example, here a solenoid to an electrically operated valve, where the initial design was deemed weak due to sensitivity for the chemical components occurring on the engine.

Figure 6 - Backshell destroyed by chemicals

As an improvement, the design was improved by adding a metallic backshell and selecting a filler material with better chemical durability.

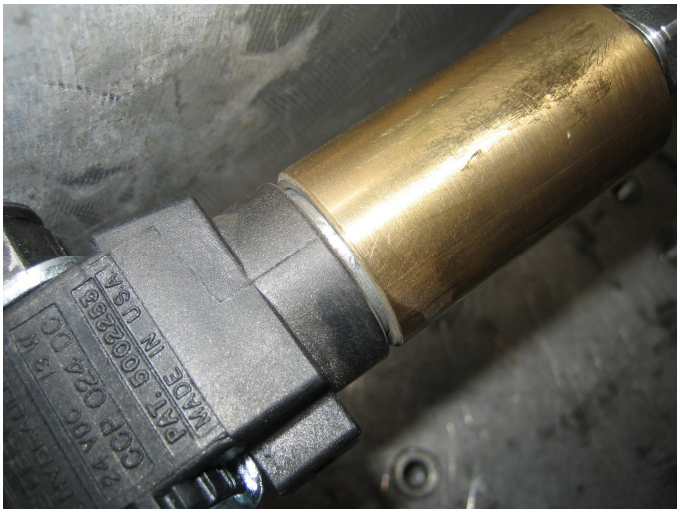

Figure 7 - Solenoid with metal backshell

This design actually survived conventional stress testing, but failed on the engine even after a rather short time. As it was rather clear that the failure mechanism was due to a combination of vibration and temperature cycling, a multiple stress method was evaluated in order to find out whether this would have caught the problem in an early stage. The vibration test along the worst axis was temporarily extended by temperature cycling with a heat-gun cyclically switching on and off. After only a short period of testing, the component failed in exactly the same way as in real operation, thereby also clearly indicating the necessity of real HALT testing.

Figure 8 - Solenoid failed after HALT test

Figure 9 - Redesigned solenoid with mechanical locking

Due to this and a number of other cases, Wärtsilä is currently extending the tests capabilities to reach a full multiple-stress capability.

Conclusions

Although experience and proven design procedures influence the reliability of the final embedded design a lot, experience has shown that certain methods clearly influence the quality of the final embedded design. Such methods involve a fully integrated tool chain, where “virtual validation” can be carried out using simulation, and complete software and hardware validation procedures, where the design thoroughly is evaluated before finalization. With these methods, the productivity of the engineering can be kept high, while guaranteeing a reliable design.

References

[1] J. Pensar, “Design of Engine Control Systems for Large Heavy Duty Applications”, SAE World Congress 2007, Detroit, paper 2007-01-1598, 2007.

[2] J. Pensar, “Engine Management And Automation – Keeping Pace With Changes”, CIMAC Congress 2007, Wienna, paper 187.

[3] A. Saikkonen and T. Kaas, “High-Level Languages in Low-Level Programming – A Case Study on the Use of Symbolic Programming and Simulation in the Development of Embedded Controls” *proceedings of Automaatio 05 Seminar Days*, Helsinki, Finland, pp. 183-188, 2005.

[4] www.mathworks.com