# Reliable SW/HW Co-Design for Wireless Communication System Integrating the Spin Model Checker and Celoxica's DK Suite

Stefanos Skoulaxinos
*Heriot Watt University*
*S.Skoulaxinos@hw.ac.uk*

## Abstract

*This paper presents the development of a wireless communication system, the RF Identification Tag, built and tested in Heriot-Watt University, Edinburgh. The design flow commences in Spin, a high level model checking tool optimized for the verification of distributed systems. The abstract software model is synthesized automatically to HDL (Verilog/VHDL) and subsequently downloaded to the targeted FPGA platform. To enhance autonomous capacity of the device, run-time fault tolerance schemes including multi-layered watchdog timers and forward error correction routines are also developed. The wireless application is finally tested under a lab emulated EMI scheme and system survivability is examined and quantified. Reliability is thus estimated and analyzed in CASRE (Computer Aided Software Reliability Estimation)developed by JPL-NASA. The principal objective of the paper and the associated research project (launched in 2002) is to investigate how a number of high-level reliability enhancement strategies can be utilized to promote more dependable embedded applications focusing primarily on the FPGA Technology.*

## 1. Introduction

Embedded systems play an increasingly significant role in our every day lives. From modest mp3 players to automotive and space exploration missions, they all entail similar technologies and tools. The design of such devices is a multifaceted process involving a number of intricate areas including hardware implementation, memory management and real time operation. Aiming to confront such low-level issues efficiently, design and debugging tends to be reasonably ad-hoc. Such informal approach can impair system testability, entangle fault removal techniques and compromise reliability. As embedded hardware implementation becomes automated, and tools operate at a more abstract level, the design lifecycle can support higher order practices such as formal methods and structured design principles. Such techniques have been proven to enhance system transparency and product quality in IT applications. Their fundamental objective is to regulate the development process and impose a precise design channel through which fault removal tools can operate optimally.

Reliability is particularly significant if the system is to be embedded at a remote location, as late modifications may not be feasible. The ID Tag, the wireless application examined in the paper, resides in this group. It is expected to operate effectively for a number of years upon its remote implantation without any form of maintenance. Aiming to accommodate such level of robustness, it is vital to ensure that adequate effort is invested towards the development of the product.

### 1.1. The problem addressed in the paper

This paper presents the utilisation of high-level reliability enhancement strategies for the tag wireless communication system. A safety-orientated design lifecycle, system modeling and verification promote early error detection and correction. Through automated code translation and hardware implementation, targeting the computation competent FPGA technology, both software and hardware failure scenarios are addressed and resolved. Furthermore, to enhance autonomous capacity and survivability of the device, a number of run time fault tolerance schemes are also developed and integrated.

### 1.2. Related Work

High order reliability enhancement methods appear to be drawing considerable attention in embedded systems and FPGAs in particular. Esterel, a successful formal verification EDA vendor with reputable wins in a number of safety critical

applications (Airbus A340, Eurocopter and Schneider nuclear power plants) currently supports automated VHDL generation in its latest Suite. This operation fabricates a path from high quality abstract design and verification to automated FPGA hardware implementation. According to embedded experts this route is likely to be followed for the development of safety critical segments of future FPGA applications (reference 16).

Xilinx, the leading provider of FPGAs is also beginning to embrace higher level practices. The company's CTO in a recent interview (Dec 04 Grenoble) consented that abstract tools are currently in the pipeline aiming to handle the increasing complexity of FPGA systems (reference 17).

## 2. Targeted Hardware – FPGA Technology Overview

Field Programmable Gate Arrays (FPGAs) is the hardware platform utilized in the application. FPGAs is a recent technological achievement introduced around 25 years ago. They were originally developed to combine the computational competence of ASICs (Application Specific Integrated Circuits) and the re-configurable feature of conventional Processor Technology.

Their internal architecture is based on hardware computational elements (logic gates) rather than the software based Digital Signal Processors (DSPs). FPGAs can operate in a truly concurrent manner enhancing operation speed even further. Those two characteristics contribute to their superior performance and make them ideal in applications where immense processing power is anticipated.

This computation-powerful technology, along with its concurrent potential have been exploited in a number of embedded applications including safety critical aerospace missions. One such example is NASA's "Spirit" and "Opportunity" Mars Rover Vehicles. FPGAs were the "main brain" of the rovers controlling motors for the wheels, steering arms, cameras, instrumentation, as well as the pyrotechnic operation during the multi-phase descent and landing.

## 3. Development Lifecycle

The development of the tag was based on a structured design methodology in order to enhance system reliability. The lifecycle (figure3) unfolds around the Spin Model Checker. Spin is considered one of the most efficient software verification tools currently available. It is actively used in mission and safety critical NASA applications such as the application to Cassini (mission to Saturn) and the Mars Pathfinder.

The lifecycle begins with requirements analysis and system specifications description in a graphical method (UML). The core of the application is subsequently designed in the Promela language. In this stage, simulation as well as verification is performed under Spin. The verified Promela model is subsequently translated to HandelC, a C based language for FPGAs and synthesis to gate-level implementation is performed. The finalized config file is downloaded to the FPGA hardware and system testing is initiated.

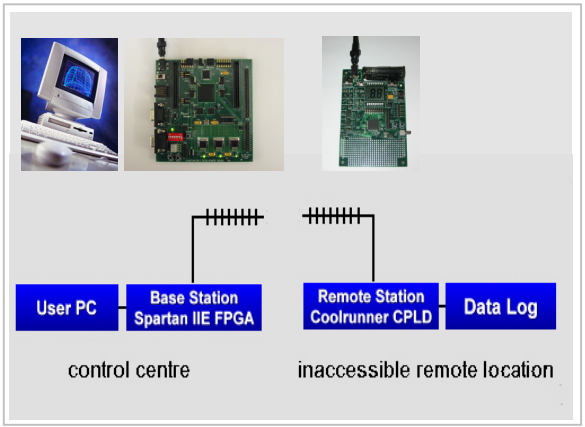



**Figure 1 LRID Tag System**

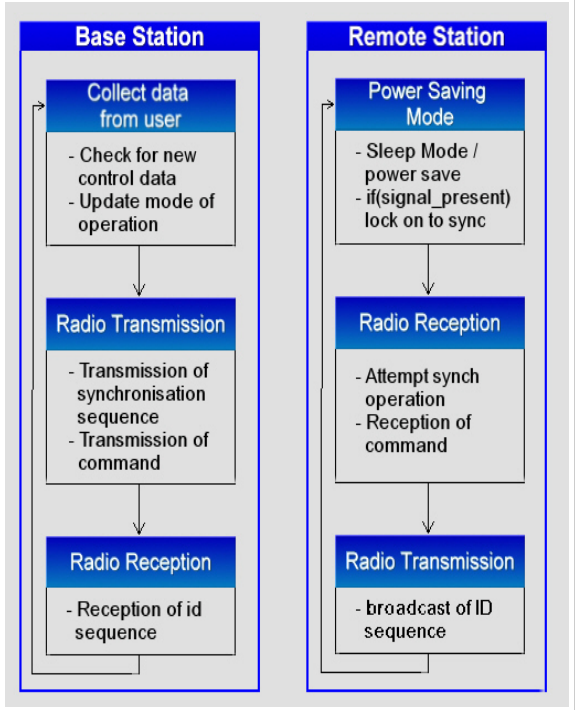



**Figure 2 Tag Operation**

## 4. The Wireless Communication System (LRID Tag)

The Tag application is composed by a base station controlled by the user and remote stations implanted in inaccessible locations. The base station initiates transmission by broadcasting a command sequence. Selected remote stations respond by transmitting a unique Identification sequence (ID) along with any data required by the base (figure 2). The time of arrival of the ID is also analyzed to establish tag location.

Base station transmission is divided into distinct phases each having different purpose and significance. In the first stage, the synchronization sequence, remote stations are stimulated to exit power-save mode and become synchronized using a variable width modulation scheme. The period of the sync signal diminishes linearly with time conveying information on command transmission schedule.

Assuming all stations are synchronized properly, the base proceeds with the transmission of the command. The command is composed by a 16 bit Manchester encoded Return to Zero Scheme with a matrix based forward error correction architecture. The sequence was designed to endure high levels of noise but also be
efficient enough for power consumption considerations.

Subsequently, the base initiates a high speed counting operation and awaits the ID and data to arrive. The time of arrival is utilized to establish Tag location. The precision of this method is highly significant and directly proportional to processing capability of the targeted Technology. In this case, the Spartan IIE FPGA can sample at 100MHz rate, providing optimal results.

On the other end, remote stations spend the majority of their life in Sleep/power-save mode. If an input signal is detected, the station locks onto the sync and subsequently collects the command. Reception is based on a multi-sampling and parity checking strategy. The station finally responds to an identified command by broadcasting its unique identification sequence.

## 5. Fault Tolerance Schemes

One of the primary objectives of the associated research project is to enhance the tag with a certain level of autonomous capacity. Stations are thus capable of withstanding increased levels of noise and regulate run-time software or hardware mal operations. The scheme utilized towards this attempt is illustrated below.

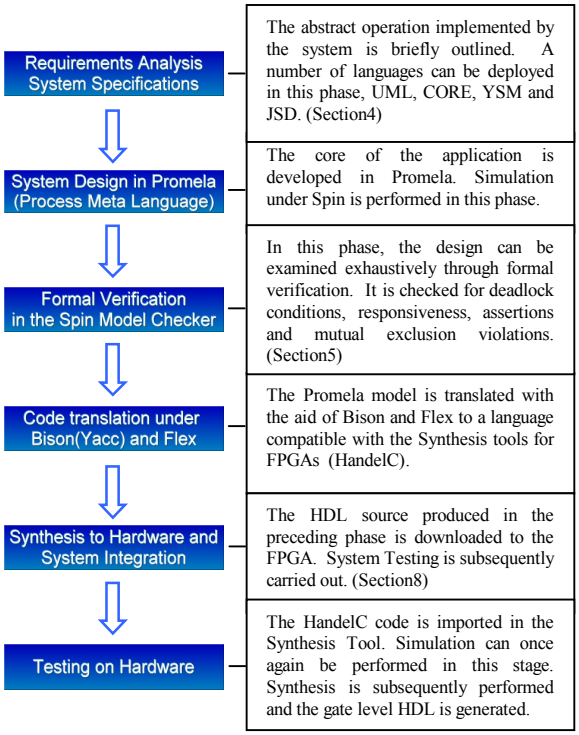



**Figure 3 Development Lifecycle**

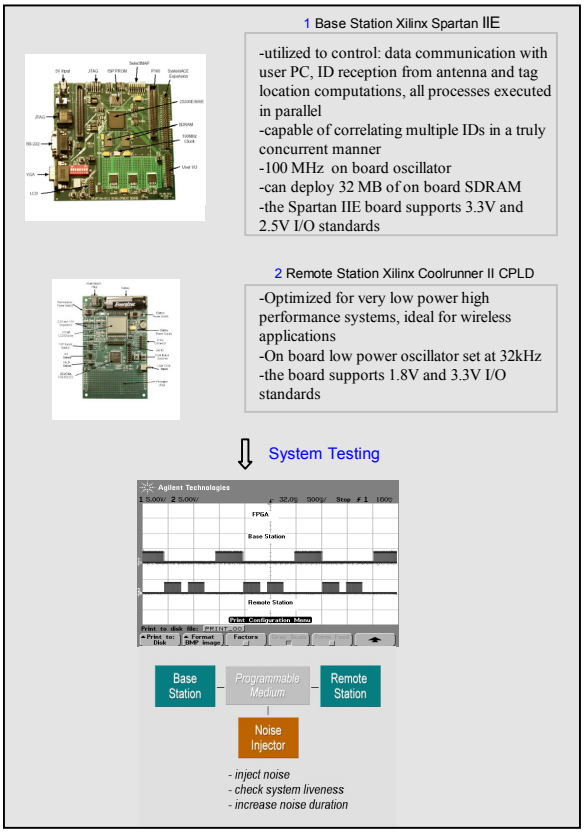



**Figure 4 Testing**

### 5.1. Forward Error Correction (FEC) – Noise Tolerance Method

The majority of digital wireless applications utilize forward error correction schemes aiming to tolerate possible transmission noise. The selection of a suitable FEC code depends on a number of conditions such as expected noise characteristics, processing capabilities and power considerations.

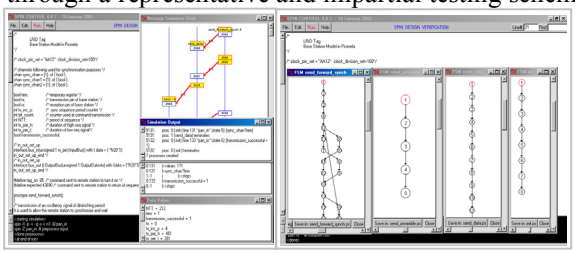
The FEC deployed in the application was based on a two dimensional matrix. The 16 command bits were placed as the matrix elements, and 8 parity bits were added as array co-ordinates. If transmission noise corrupts the command sequence, the parity scheme can be utilized to detect and correct the fault. Th FEC along with the multi-sampling strategy can assist the device to tolerate high levels of noise at run time operation. The algorithm was optimized to match power availability constraints as well as area and speed considerations of the targeted FPGAs.

### 5.2. Watch Dog Timers (WDT) – Internal Deadlock Monitoring

Due to a number of conditions (software or hardware defects) it is possible that an embedded device will hang or deadlock. As this is common in desktop PCs and a user Reset normally resolves the fault, in embedded devices an analogous automated monitoring scheme needs to be constructed. A popular embedded architecture utilized to detect and recover from such faults is Watch Dog Timers (WDTs). WDTs are hardware monitoring structures expecting to be reset by the embedded software in a periodic manner. If the system does not reset the associated WDT in time, a deadlock is assumed and exception handling routines are initiated. Typical recovery strategies for time outs involve re-attempting failed functions or performing a complete system and peripheral reset. WDTs are highly significant in safety critical applications as they form the ultimate line of defense against a system failure. They are used in a wide range of applications ranging from low budget house appliances to safety critical NASA space exploration missions.

## 6. System Testing

Following synthesis and system integration, the developed application is placed in an artificial noise injection test platform. A PIC-16F876 chip is utilized to inject predefined noise patterns to a programmable transmission medium. The noise duration is progressively increased to detect the full extent and capacity of the embedded fault tolerance schemes. System survivability of the protocol is thus quantified through a representative and impartial testing scheme.



**Figures 5 Algorithm Verification**

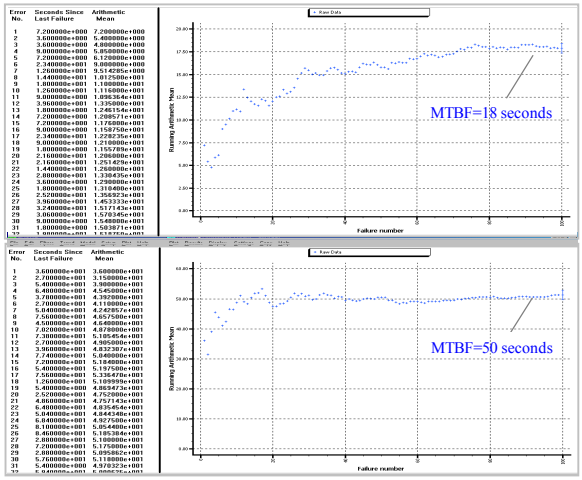



**Figure 6 Reliability Estimation**

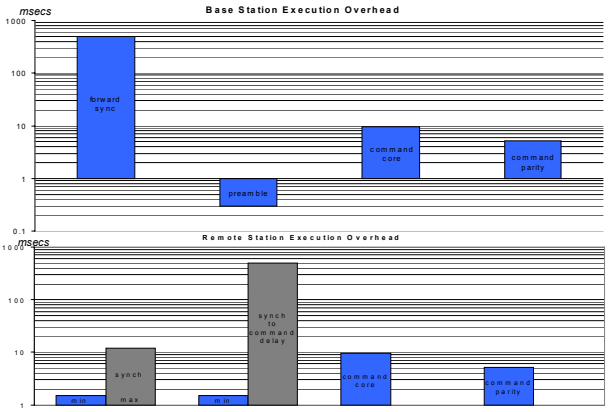



**Figure 7 Station Overhead Distribution**

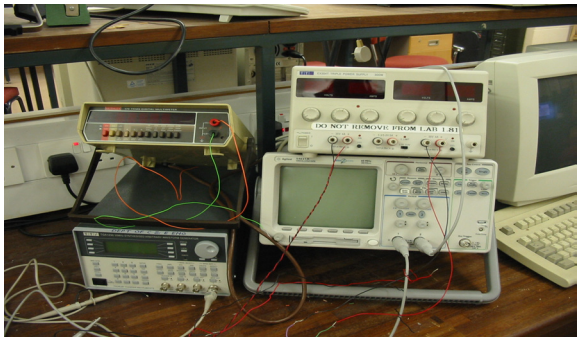


**Figure 8 Apparatus**

## 7. Test Results Analysis

Results from system testing, including mean time before failure (MTBF) in a heavily noisy environment were analyzed using CASRE 3.0 (Computer Aided Software Reliability Estimation). CASRE is developed and used by the Jet Propulsion laboratory (JPL, NASA). The results (figure 6) indicate that the FEC scheme along with multi-sampling can dramatically enhance system survivability. Note that the displayed MTBF is not to be encountered by the application under normal conditions considering that the lab emulated noise was exceptionally high.

## 8. Conclusions

This paper presented a number of compile and run-time reliability enhancement strategies for the Tag Communication System. We have illustrated the effect of these methods by testing the application under harsh environmental conditions. High level practices used in the project as well as reliability estimation procedures were proven to be highly intuitive for the application capabilities. The research team believes that abstract and formal design routes are to be embraced by an increasing number of embedded applications in the future. Such methodologies can provide the abstraction required for the development of more complex systems, and the formality for enhanced reliability and robustness.

## Acknowledgements

The author wishes to thank everyone who has contributed to the conception and development of the research project. The Dependable Systems Group and Microelectronics Group in Heriot Watt University, as well as the Institute for System Level Integration (ISLI) and Scottish Embedded Software Centre (SESC) in Livingston.

## References

[1] J. P. Calvez, “Embedded real-time systems”, Wiley, 1993
[2] S. Heath, “Embedded systems design”, Newnes, 1997
[3] D. Gray , “Introduction to the formal design of real-time systems”, Springer, 1999.
[4] J. Vytopil , “Formal techniques in real-time and fault-tolerant systems”, Kluwer 1993
[5] J.P. Tsai and others, “Distributed real-time systems: monitoring, visualization, debugging, and analysis”, Wiley, 1996
[6] S.T. Allworth and R.N. Zobel, “Introduction to real-time software design”, Macmillan, 1986
[7] M. Blackman, “Design of real time applications”, Wiley, 1975
[8] M. S. Roden., “Digital and data communication systems”, Prentice-Hall, 1982
[9] A.J. Viterbi and J.K. Omura, “Principles of digital communication and coding”, McGraw-Hill, 1979.
[10] A. Ahmed , “Data communication principles: for fixed and wireless networks”, Kluwer, 2003
[11] V. K. Garg and J. E. Wilkes, “Wireless and personal communications systems”, Prentice Hall, 1996
[12] P. Nicopolitidis and others, “Wireless networks” Wiley, 2003
[13] G. Elliott and N. Phillips, “Mobile commerce and wireless computing systems”, Addison-Wesley, 2004
[14] T. S. Rappaport, “Wireless communications: principles and practice” Prentice Hall, 1996
[15] Y.B. Lin and I. Chlamtac, “Wireless and mobile network architectures”, Wiley, 2001
[16] R. Goering, “Suite taps Esterel language's new hardware focus” , http://www.embedded.com
[17] P. Clarke, “APIs can handle FPGA Complexity, says Xilinx CTO”, http://www.embedded.com