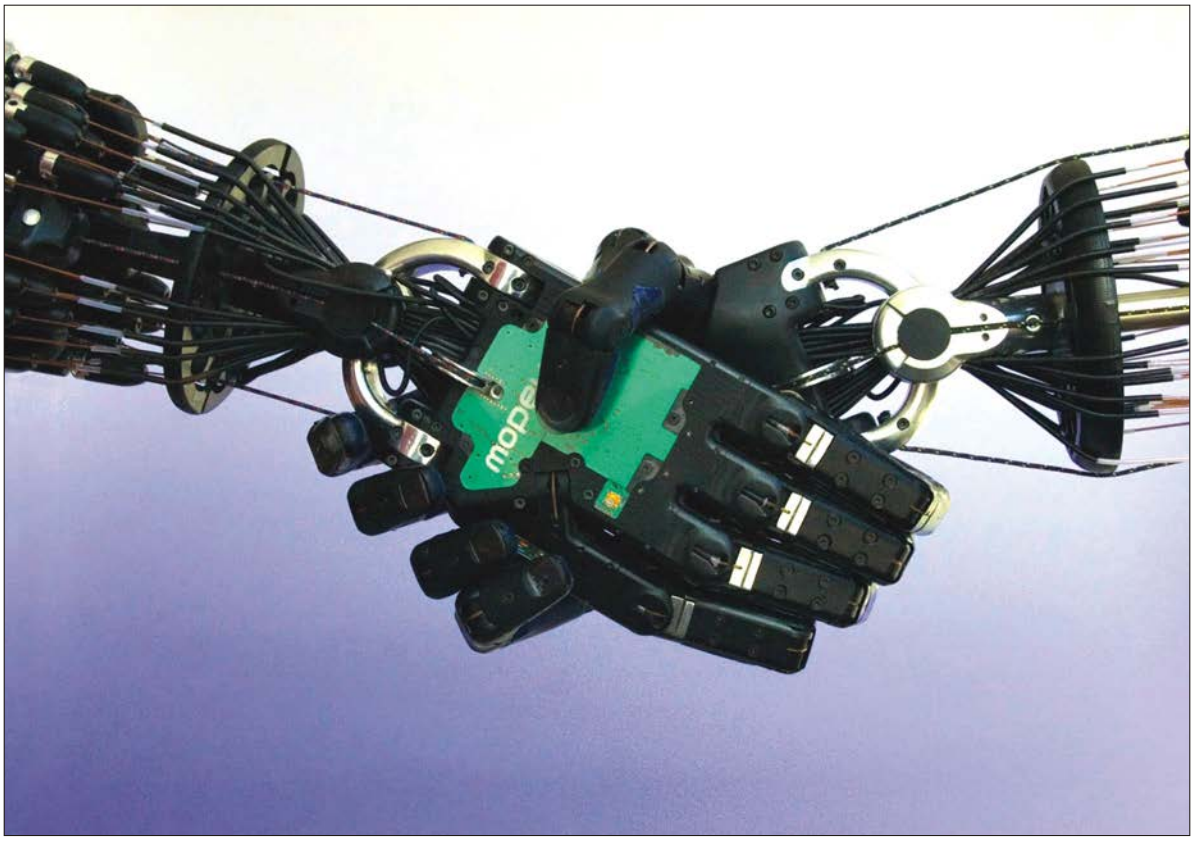

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Artificial Intelligence 5 (4): 214-220, 2012
ISSN 1994-5450 / DOI: 10.3923/jai.2012.214.220

Verification and Validation Methodology for Safety Critical Embedded Systems

P. Swaminathan
School of Computing, SASTRA University, Thanjavur, India

ABSTRACT

Embedded Systems used for control of the process plants can be classified as safety critical embedded systems. To achieve the specified probability failure on demand, it is essential to customize the relevant IEEE standards. Since the requirement specifications will be well specified for process control applications, it is appropriate to follow the waterfall product development cycle. Enough thoughts are not given for Verification and Validation of embedded systems. Verification and Validation process for safety critical embedded system and the challenges for Verification and Validation team are detailed in this study.

Key words: Process control applications, verification and validation, probability of failure on demand

INTRODUCTION

Embedded systems are increasingly used for control of the process plants. For realizing reliable operation of the embedded systems it is important to clearly specify the role of different teams. Process team will generate the system requirement specification for the embedded system. Development team will develop both the hardware and application software. The reports of Verification and Validation (V and V) team will be audited by Licensing team as explained in Fig. 1.

Embedded Systems deployed in safety critical application have to satisfy the specified probability of failure on demand (pfd). At every life cycle stage, customized IEEE standards need to be followed. Quality assurance team will ensue that the appropriate standards are fully followed at every life cycle stage of the product development cycle. Verification process ensures that design of each stage is in full compliance with the requirements of the preceding stage. Validation process will ensure that a safety critical embedded system performs satisfactorily as per the overall requirement specifications.

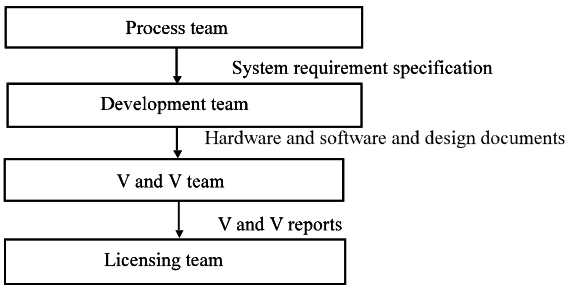

Fig. 1: Role definition for realization of safety critical embedded system

Normally enough thought is not given for Verification and Validation process. If the team members for Verification and Validation team are not properly selected and if proper methodology is not followed by Verification and Validation team, safety critical embedded systems will not perform satisfactorily (Thirugnana Murthy *et al.*, 2007). Objective of the study is to identify the challenges faced by Verification and Validation team during V and V process of safety critical embedded systems.

However, the following precautions are normally taken to ensure the specified reliability of safety critical embedded systems:

- To eliminate fuzziness in requirement specification, formal specification of requirements and appropriate testing strategies are formulated (Kloos *et al.*, 2011)
- Using models at the core of the development process provides engineers with insight into dynamics and algorithm aspects of the system. Modeller has to learn how the system works and to decide what is relevant to the model and how to do it (Marinic *et al.*, 2011). Stimulus response models are used for designing the external requirements (Sastry and Chandra, 2010)
- Designing and Development of high quality systems require that in-process Verification and Validation of design models shall be carried out and not leaving the Verification and Validation till the end of the code development (Prakash *et al.*, 2011)
- Graphical high level representation of hardware and software components by means of UML is used for code generation by renowned automated tools to eliminate errors in coding(Gargantini *et al.*, 2008).
- Validation plan is prepared clearly listing the safety test cases (Schoitsch *et al.*, 2006). Fault tree analysis should be used in building safety test cases (Siegl *et al.*, 2011)
- For effective Verification and Validation of hardware and software, simulation set-up testing process is used (Shah and Irfan, 2005)

In spite of successful verification and validation of industrial model of safety critical embedded system at factory, the system will not perform satisfactorily at the actual site. This is mainly because the interface at the input stage and the output stages of safety critical embedded system is not well defined in the requirement specification document. The electrical loading of parallel electronics of the sensor signal, current rating of final control element, electrostatic and electromagnetic noise coupled to the input signals, vibration of the system during earth quake (floor spectra) etc. are not well defined. This study focuses on these important specific issues as challenges to Verification and Validation team.

LIFE CYCLE MODEL

For safety critical embedded system, there should not be any fuzziness in the requirement specification. Normally requirement specifications are modeled in Z or B to minimize the fuzziness. The requirement specification should take into account functional aspect, reliability, user characteristics, ambience, power supply etc. (Swaminathan, 2005; Thirugnana Murthy *et al.*, 2007) Waterfall model should be used for the development of embedded system as shown in Fig. 2.

In safety critical embedded system, commercial operating system is not recommended since source code will not be available for verification and all the features of operating system are not needed. It is advantageous to develop a dedicated monitor program. The preferred software architecture is detailed in Fig. 3 (Swaminathan and Srinivasan, 1996).

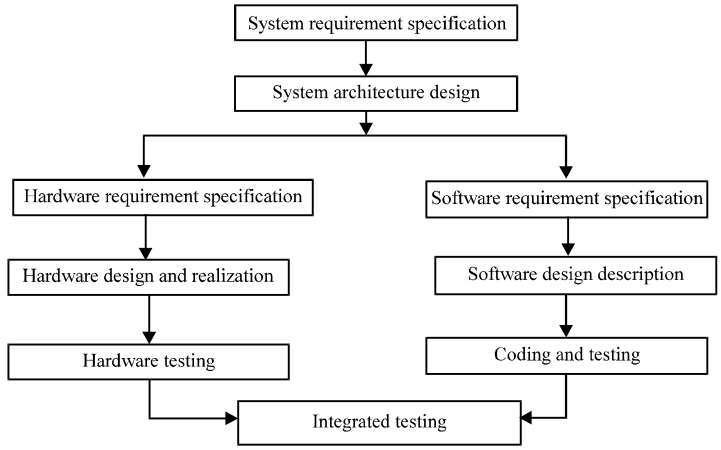

Fig. 2: Life Cycle development model for safety critical embedded system

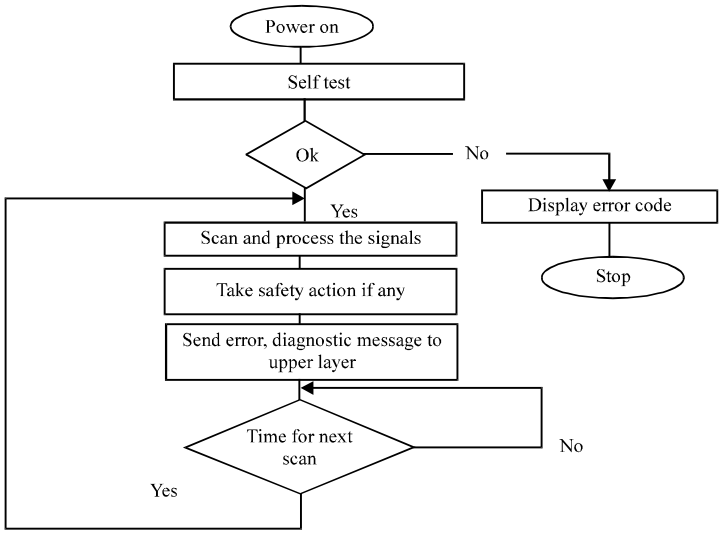

Fig. 3: Software architecture

VERIFICATION AND VALIDATION

It is very important to select correct persons as members of the Verification and Validation team. Each member shall have at least three or four years of experience in the development of similar safety critical embedded system. It is preferable to include a process specialist and a typical end user as additional members of the team.

At every life cycle stage the Verification and Validation team generates the following compliance reports:

- Compliance of system requirement specification with respect to design/control note
- Compliance of system architecture design with respect to system requirement specification
- Compliance of software requirement specification and Hardware requirement specification with respect to system architecture design and system requirement specification

- Compliance of software design description with respect to software requirement specification
- Compliance of Hardware design description with respect to hardware requirement specification
- Compliance of coding with respect to software design description
- Compliance of selection of test data with respect to detailed flow chart of the software
- Compliance of integrated test results with respect to system requirement specification

CHALLENGES TO VERIFICATION AND VALIDATION TEAM

The Verification and Validation process is never smooth. Following challenges should be tackled for generating reliable Verification and Validation reports:

- Inadequate knowledge about the process results in poor requirement specification for safety critical embedded system. This is especially true if a network of embedded systems is used for supervision and control of the process plant. Response time of sensors, scanning and processing time in the embedded systems , transmission delay of data/messages in the network and time taken by final actuating mechanism should be taken into account in the stability analysis of the computer based control system
- Lack of data regarding the electromagnetic field at different parts of the process plant will result in poor specification of EMI/EMC tests for the embedded system. The frequency range for Radiation susceptibility test should take into account the likely strength of the electromagnetic field at different areas of the process plant. It is preferable to generate this data by EM surveying at different areas in similar functional process plant. The functioning of the embedded system under test should be subjected to similar electromagnetic radiation as in Fig. 4
- Human behavior is not adequately taken into account while specifying Human Machine Interface (HMI) system. In a process plant, large number of messages regarding faulty signals need to be displayed in a limited area of graphic terminal. The methodology for displaying fault messages need to be evolved taking into account the response by the plant operator. The application software should be rugged enough to withstand the irrational data entry by operator. Detailed user manual should be prepared by Development team
- Normally requirement specification will not take into account parallel electrical loading of the input analog signals to safety critical embedded system. Misbehaviour of parallel systems will affect the performance of safety critical embedded system
- In the requirement specification, the noise (process, electrostatic, electromagnetic) in the input analog signals will not be clearly defined. A safety critical embedded system, verified in a noiseless area will not work reliably in noisy process plant

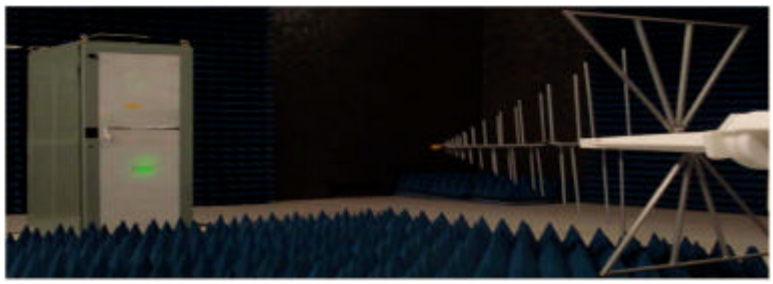

Fig. 4: Radiation susceptibility test setup

- Requirement specification will not be clear about change in sensor characteristics due to ageing. This results in unsatisfactory performance of safety critical embedded system with time
- The nature of the analog input signal due to over range will not be clearly stated in the requirement specification
- It is difficult to estimate the likely differential potential across the "ground mat" in the process plant, which will result in the circulation current in the signal lines
- The electrical power supply to embedded system will not have smooth sinusoidal waveform. Quite often spikes will be present due to switching on/off of parallel inductive loads. Functioning of the safety critical embedded system should not be affected by the presence of spikes in the power supply. Proper care should be taken in designing filters in the power supply units of embedded system. It is very important to conduct Conducted Susceptibility test as in Fig. 5
- Safety critical embedded systems are expected to perform satisfactorily even under the earthquake event. Depending upon the expected magnitude of earthquake(g),the floor spectra of the area housing the embedded system should be calculated. Representative embedded system will be subjected to simulated disturbance in a shake table as in Fig. 6 and the mechanical integrity and functional aspects should be checked
- It is very important to carry out fault/safety analysis for safety critical embedded system
- Faults can be classified as safe faults and unsafe faults. They in-turn can be classified as detectable by online diagnostics and undetectable by online diagnostics as shown in Fig. 7

Online diagnostics should be carefully designed to minimize the non-detectable unsafe faults. If probability of failure of undetectable unsafe faults is not satisfying the specified value in the Requirement specification, fault tolerant architecture should be used.

Normally triplicated system with 2/3 voting logic is used. Failure of electronic components will occur if industrial grade or mil grade components are not chosen and the embedded system is

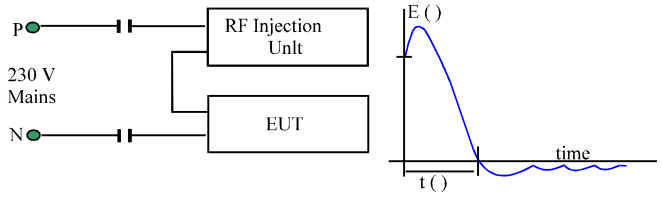

Fig. 5: Test setup for conducted susceptibility (CS) (injected spikes in the main line)

Fig. 6: Seismic test setup

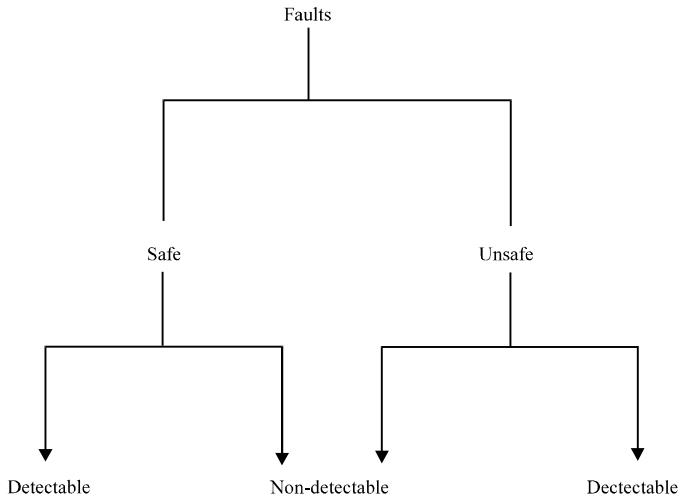

Fig. 7: Classification of faults

Fig. 8: Typical test setup for environmental testing of embedded system

subjected to dry heat or damp heat environment. Verification and Validation team should subject a representative system to dry heat and damp heat environment as in Fig. 8 in a test chamber and verify the specified functioning of the system.

Different types of failures of safety critical embedded system should be simulated to verify the safe output of safety critical embedded system (Swaminathan, 2007). Sometimes failure of memory may result in endless loop of the application software. The watchdog should time out resulting in safe output to plant.

CONCLUSION

Proper selection of the team members for the verification and validation team and well defined verification and validation process will ensure the specified performance of safety critical embedded system. But the care taken for verification and validation process during development stage of

safety critical embedded system is not applied during the Operation and Maintenance (OandM) phase. This results unreliable performance of safety critical embedded system during OandM phase of the process plant.

Separate guidelines are required for configuration management and verification and validation of safety critical embedded systems during OandM phase of process plant.

REFERENCES

Gargantini, A., E. Riccobene and P. Scandurra, 2008. A model-driven validation and verification environment for embedded systems. Proceedings of the International Symposium on Industrial Embedded Systems, June 11-13, 2008, La Grande-Motte, France, pp: 241-244.

Kloos, J., T. Hussain and R. Eschbach, 2011. Risk-based testing of safety-critical embedded systems driven by fault tree analysis. Proceedings of the IEEE 4th International Conference on Software Testing, Verification and Validation Workshops, March 21-25, 2011, Berlin, Germany, pp: 26-33.

Marinic, J., A. Mader and R. Wieringa, 2011. Validation of embedded system verification models. Proceedings of the Model-Driven Requirements Engineering Workshop, August 29, 2011, Trento, Italy, pp: 48-54.

Prakash, V.C., J.K.R. Sastry and D.B.K. Kamesh, 2011. On verification and validation of state based internal behavioral models of embedded systems. Int. J. Commun. Eng. Appl., 2: 73-85.

Sastry, J.K.R. and P.V. Chandra, 2010. A formal framework for verification and validation of external behavioral models of embedded systems represented through black box structures. Proceedings of the IEEE 2nd International Advanced Computing Conference, February 19-20, 2010, Patiala, Punjab, India, pp: 430-435.

Schoitsch, E., E. Althammer, H. Eriksson, J. Vinter, L. Gonczy, A. Pataricza and G. Csertan, 2006. Validation and certification of safety-critical embedded systems: The DECOS test bench. Proceedings of the 25th International Conference on Computer Safety, Reliability and Security, September 27-29, 2006, Gdansk, Poland, pp: 372-385.

Shah, S.M. and M. Irfan, 2005. Embedded hardware/software verification and validation using hardware-in-the-loop simulation. Proceedings of the IEEE Symposium on Emerging Technologies, September 17-18, 2005, Islamabad, Pakistan, pp: 494-498.

Siegl, S., K.S. Hielscher, R. German and C. Berger, 2011. Formal specification and systematic model-driven testing of embedded automotive systems. Proceedings of the Design, Automation and Test in Europe Conference and Exhibitions, March 14-18, 2011, Grenoble, France, pp: 1-6.

Swaminathan, P. and P. Srinivasan, 1996. Computer based core monitoring system. Proceedings of the JAERI Specialist Meeting on In-Core Instrumentation and Reactor Core Assessment, October 16-17, 1996, OECD/NEANSC, IAEA, JAERI, Japan.

Swaminathan, P., 2005. Design aspects of safety critical instrumentation of nuclear installations. Int. J. Nucl. Energy Sci. Technol., 1: 254-263.

Swaminathan, P., 2007. Modeling the Instrumentation and control systems of fast breeder nuclear reactor. Int. J. Intell. Elect. Syst., 1: 1-9.

Thirugnana Murthy, D., T. Sridevi, A. Shanmugam and P. Swaminathan, 2007. Verification and validation for safety critical real time computers. J. Intell. Elect. Syst., 1: 15-21.