Fault Injection Software Tools and Robust Design Principles for Reliability and Safety in Measurement Science Education

Lisa-Marie Faller, Hubert Zangl and Juliana P Leitzke
Institute of Smart System Technologies, Sensors and Actuators, Alpen-Adria-Universitaet Klagenfurt, Universitaetsstrasse 65-67, 9020 Klagenfurt, Austria
E-mail: lisa-marie.faller@aau.at

Abstract. In the design of measurement systems we face the fact that parameters are subject to (measurement-) uncertainties. Additionally, components may behave entirely different from what is specified, which is then considered a fault. Consequently, both uncertainty as well as probability of failure should be considered in education on robust design and reliability. In this paper we present a teaching concept based on hardware fault injection using a simple level sensor system as an example. Learning objectives are faults, errors, failures, false alarms versus misses as well as advantages and disadvantages of redundancy.

1. Introduction
In our modern society, measurement devices, i.e. sensors, the respective electronic evaluation and signal processing chains, are indispensable. Measurement science is employed to fulfill manifold tasks in consumer goods such as mobile phones and personal computers or tablets as well as in cars, (automated) production lines or safety and security systems. All electronic devices, society relies on in everyday private as well as working life, are equipped with sensors and measurements electronics. When educating engineers to become the future designers of such measurement chains, critical analysis of sensor systems with respect to robust design and reliability thus seems mandatory. It is necessary to enhance the awareness with respect to uncertainty, safety and fault handling for such systems and teach proper usage and adoption of the available methodology to prevent undesired system states. This is even more important when all of us rely on electronic measurement systems where, in, e.g., automated production chains with a cooperation and collaboration with human as well as robotic workers or autonomous vehicles, even lives depend on them.

In order to provide an introduction to the methods that are used to cope with this challenges, we provide a course on robust design and reliability for our Master students. Most of them are enrolled in the Master study program Information and Communication Engineering with a specialization in autonomous systems and robotics. It is assumed that the students are well familiar with the concept of measurement uncertainty as explained in [1], probability theory, estimation and detection theory [2] as well as electrical measurements and sensors. We consider both, qualitative and quantitative robust design methodologies [3], in order to provide a conceptual view of the topic as well as to acquaint students with the principal approach to design.
Figure 1. Coarse outline of the course on Robust Design and Reliability.

a robust measurement chain (including principles from, e.g. [4] and [5]). Fault tree analysis [6] and simulation based fault injection [7] are shown on the example of a safety critical fill level detection system.

2. General Teaching Concept
The respective course where this concept is applied is a combination of lecture and exercise under the title of robust design and reliability. A course outline is shown in Figure 1. Since this course is suggested as successor to the measurement and signal processing course where advanced stochastic concepts are covered to yield, in a certain sense, optimal estimators for measurements subject to various sources of noise, students are assumed familiar with probability theory and statistics. Hence, mathematical background to deal with measurement uncertainty is assumed known, only necessary probability distributions used to derive component failure rates are introduced at the beginning [8].

3. Principle of Fault Injection
Fault injection is a method that is widely used in evaluating the dependability of software and computer systems [7], [9] and [10]. By means of introducing faults into the system under test, error handling can be tested. However, the approach can also be used for hardware and indeed the first experiments with fault injection were proposed for hardware. As with software, the approach is used to test the dependability of the hardware system. Practically, hardware fault injection is nothing more than replacing good components in the system with faulty components, breaking connections, introducing shorts between nets and to ground. This is done in network simulations.

In order to demonstrate the idea to students, we have developed a simple Matlab toolbox for fault injection that works with the currently freely available simulator LTspice [11]. It works with the original netlist, introduces faults, calls the simulator and aggregates the results. The results are then displayed and compared to the reference. This process flow is illustrated in Figure 2.

4. Fault Injection - Educational Example
In order to emphasize the difference between faults, errors and failures as illustrated in Figure 3, as well as the concept of redundancy (e.g. [12], [13] and [14]), we use a simple measurement
system as an example and apply fault injection to it. The example application is illustrated in Figure 4 and the respective circuitry is illustrated in Figure 5. The circuitry is introduced to the students and, employing the fault injection toolbox for Matlab, the circuit-netlist is modified in order to inject faults belonging to the category of either ‘open’, ‘short’ or ‘short to ground’. Based on this first evaluation, the distinction between faults, errors and failures can be illustratively given. Also, the basis of detection for the considered system, i.e. hypothesis testing, the quality of which is characterized by its false alarm and miss rates, is explained. In a next step, redundancy concepts to aid this design in order to avoid dangerous situations, i.e. undetected excess of level (miss), are developed. For one of these extended systems, a parallel configuration, again fault injection is applied and results are illustrated using Matlab (compare Figures 6 and 7). The outcomes of the redundant and original configurations are then compared with respect to fault tolerance. While the redundant design is capable of equalizing some system faults, it is important to point out that others, such as the short to ground of the voltage source for the respective system, can not be covered.

4.1. Parallel Redundancy Concept

Since there is not just a single solution for system redundancy, it is important to point out differences and advantages as well as disadvantages of the different concepts. A simple way to system redundancy is adoption of a second system in parallel which is a duplicate of the first. This was done for the illustrating example with results shown in Figure 7. The supply voltage source is chosen to be the same for both and the connection is done via diodes, to avoid feedback. Such a parallel configuration reduces the overall miss rate and its probability of failure can be generally given as

\[ F_{par_n}(t) = \prod_{i=1}^{n} F_{simple_i}(t) \] (1)
Figure 3. Illustration of fault, error and failure as defined by the IEC 60050-191:1990 [15], compare also [3]: The error is defined as the deviation between the target and the actual system output, a failure occurs if the system output violates the pre-defined limits, while a failure, according to this definition is transient, the term fault is used to describe a static system behaviour, i.e. when the system output is out of specification and will not return to within specifications without external input (e.g. repair). While in the norm the term ‘event’ is used to describe the transient nature of failure, this is not to be confused with an event in the probabilistic sense.

Figure 4. Schematic illustration of the example application.

Figure 5. Simple (non-redundant) measurement system for illustration of fault injection. The system comprises a capacitive sensor front end, a demodulation circuitry and a trigger. If the capacitance is high due to the proximity of a liquid, the output indicates that the fill level is critical.
Figure 6. Results for the output signal as obtained using the fault injection toolbox on the non-redundant system shown in Figure 5. In the tool, the results are easily annotated by clicking on the traces. A succeeded detection is indicated by the rise of the voltage level to 5 V. System failures are caused by the faults resulting in non-rising curves (here: 16 curves).

and the reliability can subsequently be given by

\[
R_{\text{par}_n}(t) = 1 - F_{\text{par}_n}(t) = 1 - \prod_{i=1}^{n} F_{\text{simple}_i}(t)
\]  \(2\)

Assuming constant failure rates for the two parallel systems, i.e. the probability of failure follows an exponential distribution, we can find the Mean Time To Failure (MTTF), which is the expected failure time, as [16]

\[
MTTF_{\text{par}_n}(N, n) = \int_0^\infty R_{\text{par}_n}(t)dt
\]  \(3\)

With \(N\) the number of series components (of the respective subsystems) and \(n\) the number of parallel systems. As is outlined in [16] a sufficiently accurate approximation of this integral for
systems with components exhibiting identical failure rates $\lambda$ is

$$MTTF_{par,n}(N, n) = \frac{1}{(\lambda N)} \left[ 1 + \sum_{i=1}^{n} \sum_{j=1}^{i} \left( \frac{n + 1 - j}{N + j} \right) \right] 0 < n \quad (4)$$

While these calculations are valid for systems without common components, in the example system, the performance is poorer due to, e.g. the common voltage supply. In our example, the improvement in performance can be quantified by the reduction in the misses (16 versus seven) for the redundant system. This is achieved although the number of components and consequently also of possible faults is increased.

4.2. Further Take-Home-Messages

While dual (parallel) systems already provide for increased system reliability, various other configurations are possible which will add safety in critical applications. A possible alternative is to introduce parallel units with subsequent voting, so-called 'k-out-of-n' systems. Also partitioning can be adopted to build systems with redundant paths to provide increased system reliability. For all applications, the way to the design of such hierarchies should follow the 'Keep It Small and Simple' (KISS) concept. Since, although we achieve better performance in case of misses and provide for an increased MTTF, it is important to be aware of a major drawback of such extended topologies: increase in power consumption, weight and number of parts. Even for designs with dynamic redundancy, where a switch is employed to change between either of two parallel systems in case of one of them failing, additional maintenance as well as detection mechanisms are necessary.

5. Conclusion

Besides the consideration of uncertainties, robust design also has to consider possible faults. In this paper we introduce a simple toolbox for Matlab that allows to perform fault injection in spice simulations of measurement systems. Using this in a course on robust design and reliability, it is aimed to increase the awareness with respect to faults, errors and failures as well as advantages and possible shortcomings of redundancy.

References

[1] Zangl H, Zine-zine M and Hoermaier K 2015 Utilisation of software tools for uncertainty calculation in measurement science education Journal of Physics: Conference Series vol 588
[2] Kay S M 1993 Fundamentals of Statistical Signal Processing, Estimation Theory (Prentice-Hall, Inc.)
[3] Rausand M and Hoyland A 2004 System Reliability Theory (John Wiley & Sons, Inc., Hoboken, New Jersey)
[4] Brasseur G 2003 IEEE Transactions on Instrumentation and Measurement
[5] Bergman B, de Mar J, Lorn S and Svensson T (eds) 2009 Robust Design Methodology for Reliability (John Wiley & Sons, Ltd.)
[6] Dhillon B S 2007 Applied Reliability and Quality (Springer-Verlag London Limited)
[7] Benso A and Prinetto P (eds) 2003 Fault Injection Techniques and Tools for Embedded Systems Reliability Evaluation (Springer US)
[8] Kececioglu D B 2002 Reliability Engineering Handbook, Volume I (DEStech Publications, Inc.)
[9] Piscitelli R, Bhasin S and Regazzoni F 2015 Analog circuit fault simulation approach based on pspice engine 10th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS)
[10] Barenghi A, Hocquet C, Bol D, Standaert F, Regazzoni F and Koren I 2014 IEEE Transaction on Emerging Topics Comp. 2
[11] 2016 URL http://www.linear.com/designtools/software/
[12] Hecht H 2004 System Reliability and Failure Prevention (Artech House, Boston)
[13] Ushakov I A (ed) 1994 Handbook of Reliability Engineering (John Wiley & Sons, Inc.)
[14] Pham H (ed) 2003 Handbook of Reliability Engineering (Springer-Verlag London Limited)
[15] Committee I T 1990 Iec 60050-191:1990 Tech. rep. International Electrotechnical Commission
[16] Sweet A L, Lam Y and Bott J 1986 IEEE Trans. on Reliability R-35 539–540