RUPRECHT-KARLS-
UNIVERSITÄT
HEIDELBERG

International Workshop on the
Design of Dependable Critical Systems

ECOMODIS

Proceedings

of the
International Workshop on the
Design of Dependable Critical Systems
"Hardware, Software, and Human Factors in Dependable System Design"

DDCS 2009

September 15, 2009
Hamburg, Germany

In the framework of
The 28th International Conference on
Computer Safety, Reliability and Security
SAFECOMP 2009

Edited by

Achim Wagner[1], Meike Jipp[1], Colin Atkinson[2] and Essameddin Badreddin[1]

[1] Automation Laboratory, Institute of Computer Engineering, University of Heidelberg
[2] Chair of Software Engineering, University of Mannheim

International Workshop on
the Design of Dependable Critical Systems
September 15, 2009, Hamburg, Germany

Safety Recommendations for Safety-Critical Design Patterns

Ashraf Armoush and Stefan Kowalewski

Embedded Software Laboratory
RWTH Aachen University
Aachen, Germany
{armoush, kowalewski}@embedded.rwth-aachen.de

Abstract. The concept of design patterns, which is considered as one of the commonly used techniques in the development of software and hardware systems, is applicable to be used in the design of safety-critical embedded systems. While several safety metrics and assessment methods have been proposed to evaluate safety-critical systems, most of these methods cannot be used for safety-critical design patterns, due to the fact that a design pattern presents a high-level abstract solution to commonly recurring design problem and it is not related to a specific application or to a specific case. This paper proposes a system of safety recommendations for safety-critical design patterns, which can be used in the assessment of design patterns for safety-critical embedded systems to reflect the severity of failure in the target application. The proposed safety recommendations are based on the safety recommendations of the IEC 61508 standard, and contain additional 3 types of recommendations: weakly not recommend, weakly recommended, and moderately recommended.

Key words: Safety-Critical, Design Patterns, Safety Recommendations

1 Introduction

With the increasing use of the concept of design patterns as a universal approach to describe common solutions to widely recurring design problems in software and hardware domain, it has become a good candidate for the design of safety-critical embedded systems. In general, the safety-critical systems address the applications in which failure can lead to serious injury, significant property damage, or damage to the environment [1, 2]. The design of these systems should fulfill the intended functional requirements (FR) as well as non-functional requirements that define qualities of a system such as: safety, reliability, and execution time.

System safety represents the main non-functional requirement for safety-critical embedded system. It is defined by *MIL-STD-882D* standard [3] as "Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment".

Therefore, many design techniques, concepts, safety methods, metrics and standards have been proposed and used to cover the development lifecycle and to improve the non-functional requirements of such safety-critical systems.

While the commonly used standards give recommendations for safety design techniques, none of these standards gives recommendations at the level of design patterns. In most situations, design patterns present abstract solutions that combine more than single safety technique and design method to solve some common design problems. Therefore, a system of recommendations should be used for safety-critical design patterns to facilitate the comparison process and safety assessment for these patterns.

In this paper, we propose a systematic method to find safety recommendations for safety-critical design patterns. This method is based on the recommendations proposed by *IEC 61508* standard [4] for safety techniques. The proposed safety recommendations, which reflect the importance of the addressed design pattern and severity of target applications, can be used later as a part of a safety assessment method for design patterns.

2 The Concept of Design Patterns

The idea of design patterns was original proposed by the architect "*Christopher Alexander*" [5], then it became one of the widely used techniques to support designers and system architects in their choice of suitable solutions for commonly recurring design problems.

While this concept has been applied in several application domains of hardware and software design (see e.g. [6][7]), further research is still needed to adapt this concept for the field of safety-critical embedded systems. The design of these systems is considered to be a complex process, since there are many non-functional requirements, mainly safety, that have to be fulfilled by these systems to assure that the risk of hazards is acceptable low.

Due to the fact that the current representations of design patterns lack a consideration of potential side effects on non-functional requirements, we proposed in a previous paper [8] a pattern representation template for safety-critical embedded application design methods. This representation includes the traditional pattern concept in combination with an extension describing the implications and side effects of the represented design method on the non-functional requirements of the overall system.

In order to facilitate the safety comparison process between the design patterns under consideration, a system of safety recommendations for safety-critical design patterns should be constructed. Later, these recommendations can be used in a safety assessment method for safety-critical design patterns.

3 Safety Standards and Risk Metric

In the design of safety-critical embedded systems, specific aspects, requirements, techniques, and safety management have to be considered. Thus, many safety

standards have been proposed to cover the safety management of safety-critical systems throughout their lifecycles. Some of the important and commonly used standards are: *MIL-STD-882D* [3] which is a military standard, and *IEC 61508* [4] which is a well-known application-independent standard.

Most of the time, system safety is related to the risk of failure in a system and the techniques that should be used to reduce the risk to an acceptable level. The safety assessment of safety-critical systems requires the use of a specific safety and risk metric. Thus, many metrics, such as *Steady-State Safety* (S_{SS}) and *Mean Time to Unsafe Failure* ($MTTUF$) (see e.g. [9][10]), have been proposed to be used in the assessment of safety-critical systems. Nevertheless, the risk, which is defined in the standard *IEC 61508* as a combination of the probability of occurrence of harm[1] and the severity of that harm, is considered as the most generic metric that deals with a wide range of applications. The risk metric is based on the following equation:

$$R = C \times f \tag{1}$$

– R: *the risk in the system.*
– C: *the consequence of the hazardous event*[2].
– f: *the frequency of the hazardous event.*

The aim of our research is to construct a catalog of safety-critical design patterns, and to develop a safety metric similar to the metric in Equation 1. This metric will be used as a safety and risk metric for the assessments of these patterns and to give an indication about the implication and side-effects of safety-critical design patterns on system safety.

3.1 Limitations:

A design pattern represents a high level abstract solution to a commonly recurring design problem. *It is not related to a specific application or to a specific case*; thus, it is very difficult to find an actual value for both the frequency of the hazardous event (f) and the consequence of the hazardous event (C).

In order to find parameters for our metric similar to the parameters used in the original risk metric shown in Equation 1, we have proposed in a previous paper [11] a metric that reflects the idea of frequency of hazardous event.(*see Section 5*). Furthermore, to cover the other part, we propose in the next section a method that gives an indication about the severity of the hazardous event similar to the first factor.

4 Applicability to Safety Integrity Levels

The *IEC61508*, which is the most commonly-used standard in industrial applications, defined the term *safety integrity* as “probability of a safety-related system

[1] Harm: physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment [4].
[2] Hazardous Event: a situation which results in harm [4].

satisfactorily performing the required safety functions under all the stated conditions within a stated period of time". Part 4 of the standard defines 4 discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the system. These levels range from safety integrity level 1 ($SIL1$) to safety integrity level 4 ($SIL4$) where safety integrity level 4 denotes the highest level of safety integrity.

The *IEC61508* standard introduces recommendations for techniques and measures to be applied in order to avoid safety-critial failures caused by hardware or software. These recommendations are dependent on the safety integrity levels and are classified according to their importance into 4 types:

* **HR**: The technique is highly recommended for this safety integrity level.
* **R**: The technique is recommended for this safety integrity level
* –: The technique has no recommendation for or against used.
* **NR**: The technique is positively not recommended for this safety integrity level.

You have to keep in mind that the use of these recommended techniques does not give any guarantee that the final design will satisfy the required safety integrity level. However, in order to get a certificate for a specific safety integrity level, the standard should be used in the complete lifecycle of the design process.

While a safety integrity level is derived from an assessment of risk, it is not a measure of risk [12]. The safety integrity level will be used in the first component of our approach as an indication of severity of failures in the considered application after using a specific design pattern. The applications, that require high safety integrity levels, include higher severity than the applications with lower integrity levels. Thus, the intended safety integrity level for a system can be used as an indication of the possible severity and consequence of a hazardous event in that system.

Though the IEC61508 introduces recommendations for techniques and measures to avoid safety-critical failures caused by hardware or software, these recommendations are derived from safety integrity levels and given for different design techniques but not for general design patterns or architectures. Normally, a design pattern combines more than one architecture technique to improve the system safety. Therefore, we introduce a systematic method to give general safety recommendations at the level of design patterns.

Recommendations	Value
NR	0
---	1
R	2
HR	3

Table 1. Safety recommendations in *IEC 61508*

To find the recommendations of importance for a specific pattern for the safety integrity levels, integer equivalent values are assigned to the recommendations as shown in Table 1. Then the average value of the existing techniques is calculated for each safety integrity level.

The resulting average value may range between two integer numbers which makes the selection of the suitable recommendation more difficult. To solve this problem, we introduce a new system of recommendations for design patterns. These recommendations contain additional 3 types: weakly not recommend, weakly recommended, and moderately recommended. The new recommendation types are classified based on the average value as shown in Table 2.

Recommendations		Average Value (*Avg*)
NR	Not Recommended	$Avg \leq 0.4$
WNR	Weakly Not Recommended	$0.4 \leq Avg \leq 0.6$
--	No Recommendation	$0.6 < Avg < 1.4$
WR	Weakly Recommended	$1.4 \leq Avg \leq 1.6$
R	Recommended	$1.6 < Avg < 2.4$
MR	Moderately Recommended	$2.4 \leq Avg \leq 2.6$
HR	Highly Recommended	$Avg > 2.6$

Table 2. Proposed system of recommendations for design patterns

4.1 Example

The *Safety Executive Pattern (SEP)* [13], which is a large scale pattern used to provide a centralized and consistent method for monitoring and controlling the execution of a complex procedure in case of failures, includes the following design techniques: *program sequence monitoring by a watchdog*, *test by redundant hardware*, *safety bag techniques*, and *graceful degradation*. According to the *IEC 61508* standard, the recommendations for these techniques are shown Table 3.

Techniques	*SIL1*	*SIL2*	*SIL3*	*SIL4*
Program sequence monitoring (WD)	HR	HR	HR	HR
Test by redundant hardware	R	R	R	R
Safety bag techniques	---	R	R	R
Graceful degradation	R	R	HR	HR

Table 3. Safety recommendations of the used techniques in *SEP*

Conforming to Table 3, the average recommendations, which show the applicability of the safety executive pattern to be used for different safety integrity

levels, are calculated and demonstrated in Table 4. As shown in the example,

Pattern	*SIL1*	*SIL2*	*SIL3*	*SIL4*
Safety executive pattern	R	R	MR	MR

Table 4. Safety recommendations of *Safety Executive Pattern*

our approach can be used to provide an indication of the severity of failures in the required application that will use a specific design pattern, by establishing of the intended safety integrity level and by finding the recommendation for this design pattern for this safety integrity level.

5 Probability of unsafe failure

As shown previously, it is difficult to find actual values for the risk metric in design patterns since these patterns describe general abstract solutions. This part provides a brief description for the parameter that has been used in our approach to cover the second factor in the risk metric. In general, the main goal of safety design methods is to reduce the probability of unsafe failure in the considered system. Therefore, we will use the probability of unsafe failure (P_{UF}) as a part of our metric for the risk assessment. This probability will be calculated in our approach relative to the probability of unsafe failure in a *basic system* that includes a single design channel and does not include any specific safety function.

In a previous paper [11] we have proposed a metric called ***Relative Safety Improvement (RSI)***. This metric is defined as *"the percentage improvement in safety (reduction in probability of unsafe failure) relative to the maximum possible improvement which can be achieved when the probability of unsafe failure is reduced to* 0*"*.

For any design pattern, the relative safety improvement can be calculated as shown in Equation 2:

$$\begin{aligned} RSI &= \frac{P_{UF(new)} - P_{UF(old)}}{0 - P_{UF(old)}} \times 100\% \\ RSI &= (1 - \frac{P_{UF(new)}}{P_{UF(old)}}) \times 100\% \end{aligned} \tag{2}$$

- RSI: Relative Safety Improvement.
- $P_{UF(old)}$:Probability of unsafe failure in the basic system.
- $P_{UF(new)}$:Probability of unsafe failure in the design pattern.

This part of our metric can be used in the proposed approach: either through employment of a mathematical modeling for design patterns or by using simulation techniques to demonstrate the safety improvement in each design pattern.

6 Conclusion

Safety assessment in safety-critical systems design is considered as an essential step to ensure that the final system is safe. Thus, several assessment methods and standards have been proposed to cover this process. While these methods and standards present some risk metrics, none of them can be applied to safety-critical patterns that address abstract solutions to common problems instead of real systems.

In this paper, we propose a systematic method to find safety recommendations at the abstract level of safety-critical design patterns. This method is based on the recommendations proposed by *IEC 61508* standard for safety techniques. The proposed safety recommendations, which reflect the importance of the addressed design pattern and severity of target applications, can be used together with the previously proposed metric (*RSI*) as a safety assessment method for design patterns. The combination of these two parts covers the main parameters: the frequency of the hazardous events and the consequence of these events, given in the original risk metric.

While the proposed approach can be used to facilitate the comparison process between the design patterns under consideration, there are many other factors that should be taken into consideration to achieve a comprehensive comparison. These factors include, among others: reliability, costs, time overhead and maintainability.

Acknowledgment

This work was supported by the German Academic Exchange Service (DAAD) under the program: *Research Grants for Doctoral Candidates and Young Academics and Scientists.*

References

1. Knight, J.C.: Safety critical systems: challenges and directions. In: ICSE '02: Proceedings of the 24th International Conference on Software Engineering, New York, NY, USA, ACM (2002) 547–550
2. Dunn, W.R.: Designing safety-critical computer systems. Computer **36**(11) (2003) 40–46
3. : MIL-STD 882D–Standard Practice for System Safety. US Department of Defense (DOD) (2000)
4. IEC61508: Functional safety for electrical / electronic / programmable electronic safety-related systems. International Electrotechnical Comission (1998)
5. Alexander, C.: A Pattern Language: Towns, Buildings, Construction. Oxford University Press, New York (1977)
6. Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., Stal, M.: Pattern-oriented software architecture: a system of patterns. John Wiley & Sons, Inc. New York (1996)

7. Gama, E., Helm, R., Johnson, R., Vlissides, J.: Design Patterns: Element of Reusable Object-Oriented Software. Addison-Wesley, New York (1997)
8. Armoush, A., Salewski, F., Kowalewski, S.: Effective pattern representation for safety critical embedded systems. In: 2008 International Conference on Computer Science and Software Engineering. Volume 4., IEEE CS (Dec. 2008) 91–97
9. DeLong, T., Smith, D., Johnson, B.: Dependability metrics to assess safety-critical systems. IEEE Transactions on Reliability **54**(3) (2005) 498–505
10. Yu, Y., Johnson, B.: The quantitative safety assessment for safety-critical software. In: Proc. 29th Annual IEEE/NASA Software Engineering Workshop. (2005) 150–162
11. Armoush, A., Beckschulze, E., Kowalewski, S.: Safety assessment of design patterns for safety-critical embedded systems. In: 35th Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2009), IEEE CS (Aug. 2009)
12. Redmill, F.: Iec 61508: Principles and use in the management of safety. IEE Computing and Control Engineering **9**(10) (1998) 205–213
13. Douglass, B.: Real-Time Design Patterns. Addison-Wesley, New York (2003)