Reliability Calculation of HDL-Designs for FPGA-Based Safety Related Systems

BASHIER MACHMUR
University of Kassel
Department of Computer Architecture and System Programming
Wilhelmshöher Allee 71, 34121 Kassel
GERMANY
bashier.machmur@uni-kassel.de

ALI HAYEK & JOSEF BÖRCSÖK
University of Kassel
Department of Computer Architecture and System Programming
Wilhelmshöher Allee 71, 34121 Kassel
GERMANY
ali.hayek@uni-kassel.de, j.boercsoek@uni-kassel.de

Abstract: For the use of Field Programmable Gate Array (FPGA) in safety-related applications, Hardware Description Languages (HDL) are used to define the digital function. The process of such development is presented in the international standard IEC 61508, which introduces guidelines and calculations to achieve a specific Safety Integrity Level (SIL). However, it is not concerning the estimation and calculation of the reliability of used HDL codes. In this paper, a novel reliability model for the quantitative evaluation of the reliability of HDL Designs is introduced. An example of the quantitative reliability calculation of the digital circuit design is described with the inclusion of multiple errors within a failure to validate the new approach of the reliability model for HDL. For this, conventional software reliability models (SRMs) are applied. Due to the parallel processing nature of HDL more concurrent faults can lead to a failure, therefore current SRMs need to be extended. Specifically, the comparison between the classical programming languages (CPL) based on a single error, and the HDL description with the multiple errors are represented. The results of the CPL and HDL are analyzed according to the differences, which are caused by the approach of the adaptation of the SRMs. Reliability corruption that results from the calculation of the single error is corrected by the multiple errors for the HDL. This allows the validation of the new approach of the reliability model of HDL with the existing SRMs of CPL.

Key–Words: Safety-Related Applications, IEC 61508, Hardware Description Language (HDL), Reliability, FPGA

1 Introduction

HDLs, such as VHDL and Verilog are used in electronic design automation to describe digital functions for FPGA. FPGA are used in many electronic devices like in real time systems or high performance computers [1] [2]. These FPGAs can be configured with all kinds of digital functions, which are often designed for flexible model series. Especially for low production volume, there are cost reduction compared to ASICs or discrete circuits [2]. Through the multifunctionality, parallel function execution and computing power, FPGAs leads to high performance.

For the use of FPGAs for safety related systems, special international standards like IEC 61508 are used [3] [4]. According to a given SIL, specific guidelines and measures are given, which must be fulfilled for the use of the targeted FPGA. These measures vary from on-chip redundancy and monitoring components to coding rules and testing methodologies, but don’t consider the calculation of the reliability of the used HDL Code itself. While several standards can be applied to calculate the reliability of the used hardware resources, there is almost no detailed analysis and research works concerning the reliability calculation of given HDL designs. Therefore, new research works have to be done, in order to cover the reliability of the entire safety-related system. The estimation of the reliability of the HDL design should result in a quantitative value which can be added to the system reliability value. Furthermore, future prognosis should be determined, how long the HDL Design must be tested to achieve certain reliability.

In this paper, a novel reliability model for the estimation and calculation of the reliability value of HDL designs is presented. An example of the quantitative reliability calculation of the digital circuit design is described with the inclusion of multiple errors within a failure to validate the new approach of the reliability model for HDL. Specifically, the comparison between the conventional programming languages (CPL) based on a single error, and the HDL description with the multiple errors are represented. This allows the validation of the new approach of the reliability model of HDL with the existing SRMs of CPL.
The reliability model can be used as a proof of the reliability for the safety related system.

In section 2 the novel reliability model for HDL is presented. The validation of the reliability model is introduced in section 3. Finally, in section 4, the conclusion is given.

2 The novel Reliability Model for HDL

Digital circuit design is performed in HDL and has the same requirements as CPL. For CPL, SRMs exist for estimating the failure intensity [7], [8]. These models are considered for the proposed research approach to calculate the failure intensity of the circuit design, which is described in HDL. Nevertheless, there are differences between CPL and HDL that must be included in the SRMs.

2.1 Difference between CPL and HDL

SRMs have been developed specifically for CPL that performs their processing in a sequential manner. Figure 1 represents the set of instructions in a rectangular area, which are executed sequentially. The instruction point indicates the currently executing instruction that moves through the instruction area. The sequential processing of instructions is based on CPL, such as C++ or Java. If the instruction point reaches the fault area, the system leads to a failure, because of the fault. In the fault area, the fault must be detected and eliminated. That means that one failure is caused by one fault. The SRMs are based on this assumption, which can be used for CPL.

However, HDL designs are executed in a parallel manner. Each module of a HDL design executes its function simultaneously. There are several instruction points and instruction area as shown in Figure 2. Each instruction area is stimulated by the environment and delivers the results to the other modules. So each instruction point depends on the remaining instruction points and their output values. If one of the instruction points leads to a failure, the fault has to be detected and eliminated in the instruction area. However, since the faulty instruction point depends on the remaining instruction point, there fault areas have to be examined, too. The failure may come from another instruction area that delivered faulty outputs, which led to a failure. When a failure occurs, all fault areas have to be investigated for faults. A result can be that a failure comes from more than one fault area, which delivered simultaneous incorrect results to the other instruction area. This enables multiple fault detections and corrections, which caused the failure.

As already mentioned SRMs are not made for multiple fault correction, which falsifies the results [7], [8]. For CPL the assumption is given that a failure is caused by a fault. For HDL the assumption is no longer fulfilled, since one failure is occurred through multiple faults, because of simultaneous execution of multiple modules. These differences have to be adopted into the SRMs, in order to not falsify the calculation of reliability.

2.2 Investigation of the basic assumption

SRMs are used to calculate the reliability of CPL. This models attempt to explain the behavior of the number of failures $M(t)$, which denote failure experienced by time $t$ the following characteristic:

\[
M(t) := \sum_i \delta(T_i \leq t)
\]

\[
\delta(T_i \leq t) = \begin{cases} 
1, & \text{when } T_i \leq t \\
0, & \text{else}
\end{cases}
\]  

(1)

The counting process $M(t)$ is only for the case to correct one fault, when a failure occurs. $T_i$ is a random variable representing the i-th failure time. The $M(t)$ process increases his value by 1 whenever a failure appears. Each SRM has a certain functional form of $M(t)$. The mean value function specifies the expected number of failures in the model and is defined as:

\[
\mu(t) = E(M(t))
\]  

(2)

The failure intensity function is denoted by $\lambda(t)$ . This is the current rate of change of the expected number...
of failures in relation to the time. The failure intensity function $\lambda(t)$ is obtained by differentiation of $\mu(t)$ over the time $t$.

$$\lambda(t) = \frac{d\mu(t)}{dt}$$  \hspace{1cm} (3)

The specification of the mean value function is the subject of many scientific researches, using the Markov process [11]. A Markov process has the property that the future of the process depends only on the current state and is independent of the past. This assumption is reasonable for the consideration of software failures, because the software is mainly dependent on the remaining faults. If a process $U(t)$ exists, than the probability of $U(t + \Delta t) = j$ is given in the following equation [9], [10].

$$P(U(t + \Delta t) = j) = \sum_i p_{ij}(t, \Delta t) \cdot P(U(t) = i)$$

$$= p_{ij} \cdot P(U(t) = i) + p_{jj} \cdot P(U(t) = j)$$  \hspace{1cm} (4)

Figure 3 shows the graphical representation. This model consider only the variant that one fault is responsible for the failure. Therefore it exist only two conditions for the Markov process.

For HDL several faults can be responsible for the failure. This changes the $M(t)$ process, since several faults can be corrected at a time. The modification of $M_{HDL}(t)$ process has now step sizes that can be greater than 1.

$$M_{HDL}(t) := \sum_i \delta(T_i \leq t)$$

$$\delta(T_i \leq t) = \begin{cases} 1, 2, ..., & \text{when } T_i \leq t \\ 0, & \text{else} \end{cases}$$  \hspace{1cm} (5)

Also, the Markov process $U_{HDL}(t)$ is adapted for HDL, as shown in Figure 4, with the following characteristic:

$$P(U_{HDL}(t + \Delta t) = j) = \sum_{k=0}^{\infty} p_{(j-k)j}(t, \Delta t) \cdot P(U_{HDL}(t) = j - k)$$

$$= p_{jj} \cdot P(U_{HDL}(t) = j) + p_{(j-1)j} \cdot P(U_{HDL}(t) = j - 1) + ...$$  \hspace{1cm} (6)

The Markov process consists of several conditions to adjust the SRM for HDL.

### 2.3 Specification of the Reliability Model

The numbers of the corrected faults are associated in the test procedure with the related failure times. The final results after the test execution are the failure times and the number of corrected faults.

$$T_{HDL} = \begin{Bmatrix} T_1 & F(T_1) \\ T_2 & F(T_2) \\ ... & ... \\ T_n & F(T_n) \end{Bmatrix}$$  \hspace{1cm} (7)

The failure times are represented with $T_i$ and the corresponded number of corrected faults with $F(T_i)$. For the entire failure times $T_{HDL}$ consisting of all the numbers of faults $F(T_i)$, several parts of failure times $T_{HDL}(F)$ are formed. Each part of the failure times $T_{HDL}(F)$ contains the same number of faults $F$. Each part of the failure times are considered separately for the calculation of the failure intensity with a one step of number of failures $M(t)$.

$$T_{HDL}(F) = \begin{Bmatrix} T_{F,1} & F \\ T_{F,2} & F \\ ... & ... \\ T_{F,n} & F \end{Bmatrix} \text{ with } F = \text{constant}$$  \hspace{1cm} (8)

The counting process $M(t)$ for the respective number of faults is shown in Figure 5. The sub-counting pro-
Recent Advances in Financial Planning and Product Development

![Figure 6: The Markov Process $U_{HDL_F}(t)$ depending on the corrected faults](image)

The Markov process $M_{HDL_F}(t)$ is divided in the number of the corrected faults $F(T_i)$ and is derived from the counting process $M(t)$. Each sub-process $M_{HDL_F}(t)$ contains a step size of 1. Since each step represents the same number of corrected faults, the mean value function must be multiplied with $F(T_i)$. Through this measure of the sub-counting process $M_{HDL_F}(t)$, the SRMs can be used for the calculation of the reliability for each number of faults.

### 2.4 Subdivision of the Markov process

The Markov process $U_{HDL_F}(t)$ considers each sub-counting process $M_{HDL_F}$ individually. The various conditions from Figure 4 can be divided into sub-conditions. Now there are two conditions for the Markov process $U_{HDL_F}(t)$, which is expected by the SRMs.

All the failure times with the same corrected numbers of faults get his own $U_{HDL_F}(t)$ process as a step function with the step size of 1, which is depending on the fault $F$. Through this method of subdivision of the counting process $M_{HDL_F}(t)$ and Markov process $U_{HDL_F}(t)$, the possibility is given to use the SRMs for HDL. According to the definition of SRMs, there are now only two conditions for $M_{HDL_F}(t)$ and $U_{HDL_F}(t)$ process. To calculate the reliability of HDL, the subdivisions are presented to allow the use of the SRMs, since the basic assumptions and requirements for the use of the models are now met.

### 2.5 Merging of the subdivision

Each $M_{HDL_F}(t)$ is used to calculate the mean value function $\mu_F(t)$ and the failure intensity function $\lambda_F(t)$ from the SRMs. The mean value function corresponds to the expected value of the counting process:

$$\mu_F(t) = E(M_{HDL_F}(t))$$  \hspace{1cm} (9)

Since $M_{HDL_F}(t)$ has a step size of 1, but $F$ faults are corrected per failure, the result of the mean value function $\mu_F(t)$ have to be multiplied with $F$. The result is the valid mean value function $\tilde{\mu}_F(t)$ of the number of the corrected faults $F$.

$$\tilde{\mu}_F(t) = F \cdot \mu_F(t) = F \cdot E(M_{HDL_F}(t))$$  \hspace{1cm} (10)

The total mean value function $\mu_{HDL}(t)$ is obtained by adding all valid mean value functions $\mu_F(t)$ together. The sum of all sub-processes brings back the entire process [12]. This brings the total intensity function $\lambda_{HDL}(t)$ of the HDL description:

$$\lambda_{HDL}(t) = \frac{d\mu_{HDL}(t)}{dt} = \sum_{F=1}^{\infty} F \cdot \frac{d\mu_F(t)}{dt}$$  \hspace{1cm} (11)

The reliability for HDL is given then in the following equation:

$$R_{HDL}(t) = \exp \left( - \int_0^t \lambda_{HDL}(x) \, dx \right)$$  \hspace{1cm} (12)

By derivation, the use of SRMs for multi fault correction is adjusted. By the property of parallelism of the HDL, the multiple fault correction during a failure time is given. Through the described method the reliability of HDL can be given with the use of the modified SRMs.

### 2.6 Practical Environment

The mathematical point of view to calculate the failure intensity of the circuit design based on hardware description language is presented. For the practical application a practical environment is needed. The transformation of the mathematical perspective, like what has been described in this paper, is given in the figure 7. This practical environment gives the possibility to indicate the failure intensity of the circuit design implemented in hardware description language with less effort. The practical environment system gets the Module, implemented in hardware description language and the Test Matrix over the network interface from a host system. The Module is compiled and configured in a test board with a FPGA. A microprocessor on the test board starts testing the circuit design on the FPGA. An interface is connected...
between the microprocessor and the FPGA. The inputs of the Test Matrix are given over the interface to the FPGA. The circuit design in the FPGA performs the function and returns the results to the outputs. The microprocessor compares the outputs of the Module and the Test Matrix automatically and shows the errors. In the same time the failure times are saved in the microprocessor. In addition to the failure times the microprocessor can calculate the failure intensity automatically using all Software Reliability Models and can give the best result for the circuit design. From the failure intensity the Reliability and the Mean Time to Failure can be calculated as described above in this paper. So the developer gives the practical environment system only the circuit design as a module and the Test matrix. When the microprocessor shows error in the circuit design, the developer has to correct the module and start the test again.

3 Validation of the Reliability Model

For the execution of the validation in practical, realistic failure times of HDL description are needed. The previous section represents the procedure to generate from an existing HDL description realistic failure times by dynamic tests. Through the dynamic tests, failure times with the number of corrected faults are generated and prepared for the further calculations.

Through the dynamic tests, there are $i = 173$ failures in a total test time of $t_e = 2337.63h$. During simultaneous execution, 114 single faults, 41 double faults and 18 triple faults are detected and corrected. From all SRMs, the Jelinski-Moranda Model [7] from the finite category is selected through the calculation of the Likelihood Ratio and the U-Plot methods [14].

$$\mu(t) = E(M(t)) = \mu_0 [1 - \exp(-\phi \cdot t)] \quad (13)$$

3.1 Classical Programming Language (CPL)

Primarily the calculation of the reliability for the case of the single faults for the CPL is taken into consideration. Thereby the same failure times are used for the single and multiple faults for the calculation of the SRM, with the exception that the number of corrected faults are not considered for the CPL. For each failure time $T_i$ a one-fault correction is assumed with $F(T_i) = 1$. Therefore the approach of adapting will be ignored for the following calculation, so the failure times of CPL correspond to the existing SRM. From the failure times $T_{CPL}$, the mean value function $\mu_{CPL}(t)$ of the Jelinski-Moranda Model is calculated. The parameter $\mu_0$ (Total Number of Faults) and $\phi$ (Proportionality Constant) are estimated by the Maximum-Likelihood Method [15].

$$\mu_{CPL}(t) = 173.7 \cdot [1 - \exp(-0.0021199 \cdot t)] \quad (14)$$

3.2 Hardware Description Language (HDL)

For the calculation of the reliability of the digital circuit design of the HDL description, the number of corrected faults within a failure is considered. As a result the invalid mean value function $\mu_{MF}(t)$ and the mean value function $\mu_{HDL}(t)$ of the HDL will be specified and compared with the mean value function $\mu_{CPL}(t)$ of the CPL. This allows the validation of the new concept of the reliability model for HDL with the existing SRM of CPL.

The failure times $T_{HDL}$ are divided in parts of failure times, depending of the number of corrected faults $F(T_i)$. For further calculations the i-te failure intervals $\Delta T_{F,i}(T_a, T_b), i = 1, 2, \ldots$ are required, which can be derived from transformation of the failure times $T_{HDL}(F)$ [15]. Each part of the failure times $T_{HDL}(F)$ are considered separately to calculate the corresponding mean value function $\mu_{E}(t)$.

For the case $F = 1$ the part of the failure times $T_{HDL}(1)$ is taken into an account. After the calculation of the Jelinski-Moranda Model, the following results are given:

$$\mu_1(t) = 115.96 \cdot [1 - \exp(-0.0016469 \cdot t)] \quad (15)$$

The mean value function $\mu_1(t)$ in this case corresponds to the valid mean value function $\mu_1(t)$, since in each failure one fault is corrected.

For the case $F = 2$, the following results are given for the Jelinski-Moranda Model:

$$\mu_2(t) = 41.2 \cdot [1 - \exp(-0.003377 \cdot t)]$$
$$\mu_2(t) = F \cdot \mu_2(t) = 2 \cdot 41.2 \cdot [1 - \exp(-0.003377 \cdot t)] \quad (16)$$

The valid mean value function $\mu_2(t)$ is multiplied by the number of corrected faults $F = 2$, because two faults are corrected within a failure.
For the case $F = 3$, the following results are given:

$$
\mu_3(t) = 18.8 \cdot [1 - \exp(-0.0046048 \cdot t)]
$$
$$
\mu_3(t) = F \cdot \mu_3(t) = 3 \cdot 18.8 \cdot [1 - \exp(-0.0046048 \cdot t)]
$$

The mean value function $\mu_3(t)$ must be multiplied by the number of corrected faults $F = 3$ to indicate the valid mean value function $\mu_3(t)$.

### 3.3 Validation of the Results

For the comparison, the mean value functions are considered. It will be discussed whether the new approach of the adaptation of the SRM for the HDL is justified. A feature of the validation of the adaptation is to compare the mean value function of the CPL (EF) with the invalid mean value function of the HDL (MF). For the invalid mean value function of the HDL, the multiplication with the number of corrected faults is not considered, like for the existing SRM for CPL. While both mean value functions for HDL and CPL are derived using different calculations, both functions must show similar pattern to validate the new approach of adaptation.

The mean value function $\mu_{CPL}(t)$ of CPL is given in the equation 14. The invalid mean value function $\mu_{MF}(t)$ of HDL results from the addition of the invalid mean value function $\mu_F(t)$ of the sub functions depending on the number of corrected faults.

$$
\mu_{MF}(t) = \sum_{k=1}^{3} \mu_F(t) = \mu_1(t) + \mu_2(t) + \mu_3(t)
$$

$$
\mu_{MF}(t) = 115.96 \cdot [1 - \exp(-0.0016469 \cdot t)] + 41.2 \cdot [1 - \exp(-0.003377 \cdot t)] + 18.8 \cdot [1 - \exp(-0.0046048 \cdot t)]
$$

If the number of corrected faults $F$ are included in the calculation, the valid mean value function $\mu_{HDL}(t)$ of the digital circuit design of the HDL description is given in equation 19.

$$
\mu_{HDL}(t) = \sum_{k=1}^{3} F \cdot \mu_F(t) = 1 \cdot \mu_1(t) + 2 \cdot \mu_2(t) + 3 \cdot \mu_3(t)
$$

$$
\mu_{HDL}(t) = 1 \cdot 115.96 \cdot [1 - \exp(-0.0016469 \cdot t)] + 2 \cdot 41.2 \cdot [1 - \exp(-0.003377 \cdot t)] + 3 \cdot 18.8 \cdot [1 - \exp(-0.0046048 \cdot t)]
$$

### 3.4 Reliability calculation of the HDL

From the results of the previous sections of the reliability model, the quantitative reliability of the HDL description can be calculated. Through the new adoption of the multiple faults, the failure rate $\lambda_{HDL}$ of the digital circuit design can be specified to calculate the quantitative reliability function $R_{HDL}(t)$.

The derivation of the mean value function $\mu_{CPL}(t)$ is the failure intensity $\lambda_{CPL}(t)$ of the CPL.

$$
\lambda(t) = \frac{d\mu(t)}{dt} = \mu_0 \phi \exp(-\phi t)
$$

$$
\lambda_{CPL}(t) = 173, 7 \cdot 0, 0021199 \cdot \exp(-0, 0021199 \cdot t)
$$

The last failure $i = 173$ of the test procedure indicates the end of the testing phase with $t_e = 2337, 63h$. With the end of the testing phase, the operation phase begins with the execution of the digital circuit design in a reconfigurable system. The possibility of fault correction is not given in the operation phase, which brings the result of a constant failure rate $\lambda_{CPL}$.

$$
\lambda_{CPL} = \lambda_{CPL}(t_e) = 0, 0026
$$

Through the use of the constant failure rate $\lambda_{CPL}$ the function of the quantitative reliability $R_{CPL}$ is given for CPL.

$$
R_{CPL}(t) = \exp(-0, 0026 \cdot t)
$$

![Figure 8: Mean Value Function of $\mu_{CPL}(t)$ (EF), $\mu_{MF}(t)$ (MF) and $\mu_{HDL}(t)$ (HDL) in comparison](image-url)
Recent Advances in Financial Planning and Product Development

Figure 9: Reliability Function $R_{CPL}(t)$ (EF) and $R_{HDL}(t)$ (HDL) in comparison

Further the reliability function $R_{HDL}(t)$ is calculated for the case of multiple faults for the HDL description and compared with the case of single faults of the CPL.

$$
\lambda_{HDL}(t) = \sum_{k=1}^{3} F \cdot \lambda_F(t) = 1 \cdot \lambda_1(t) + 2 \cdot \lambda_2(t) + 3 \cdot \lambda_3(t)
$$

For HDL the new approach fixes the distortion which results from the reliability function $R_{CPL}(t)$ of the CPL.

Therefore the calculated reliability function $R_{HDL}(t)$ of the HDL description reflects the real reliability value of the digital circuit design for the reconfigurable system in practice. The calculation of the difference $\Delta R(t) = R_{EF}(t) - R_{HDL}(t)$ shows a maximum distortion of 18%, what is enormous for the use in safety critical systems, if the number of corrected faults is not considered.

4 Conclusion

In this paper the method to calculate the reliability of a HDL Design was presented. The new approach of the reliability model introduces the calculation of the reliability of the HDL using existing software reliability models (SRMs). SRMs need failure times to give a quantitative value for the reliability. For this aim, FPGA based HDL designs are used to collect the failure times. Through test cases, failures are detected in the FPGA design. Parallel processing nature of HDL leads to a situation where more faults are to be corrected during a failure. This is not considered in conventional SRMs. The method of subdivisions of HDL processes, presented in this paper, gives the opportunity to use SRMs for HDL. Therefore, the counting process and the Markov process are divided depending on the number of corrected fault during a failure. Each counting process uses SRMs to calculate the mean value function for a constant number of corrected faults. All valid mean value function must be added together to get the total mean value function that leads to the intensity function $\lambda_{HDL}(t)$ of the HDL Design. With this total intensity function the quantitative reliability and the Mean Time to Failure of the HDL is specified.

The Figure 9 presents the comparison of the reliability functions $R_{CPL}(t)$ of the CPL and the reliability function $R_{HDL}(t)$ of HDL. The reliability function of the CPL shows as expected a better reliability compared to the reliability function of the HDL, since incorrectly one faults is corrected per failure. For the reliability function $R_{HDL}(t)$ of the HDL the correction of one fault per failure is not fulfilled, because of the simultaneous execution of the digital circuit design and takes the number of corrected faults into account, which is a multiple of the single faults. This means that the reliability function $R_{HDL}(t)$ of HDL is always below of the reliability function $R_{CPL}(t)$ of the CPL. Through the reliability $R_{HDL}(t)$ model
tion is to compare the mean value function of the CPL with the invalid mean value function of the HDL. For the invalid mean value function of the HDL, the multiplication with the number of corrected faults is not considered, like for the existing SRM for CPL. While both mean value functions for HDL and CPL are derived using different calculations, both functions must show similar pattern to validate the new approach of adaptation. The mean value functions $\mu_{CPL}(t)$ of CPL and the invalid mean value function $\mu_{MF}(t)$ of HDL show as expected a similar behavior by using the same assumption for the calculation. The validation shows that the approach of the adaptation is justified, because both functions are assumed with $F = 1$. For the mean value function $\mu_{HDL}(t)$ of the HDL, the number of corrected faults $F(T_i)$ is considered in the calculation.

This method can be used as a proof of the quantitative value of the reliability for the HDL function in FPGA for safety related systems. Through the reliability model future prognoses of test times can be made to achieve certain reliability.

References: