Fault-Injection Testing: FIT-Ability, Optimal Procedure and Tool for FPGA-Based Systems SIL Certification

V. Kharchenko[1,3], V. Sklyar[1,3], O. Odarushchenko[2], A. Ivasuyk[2]
[1]National Aerospace University named after N.E. Zhukovsky "KhAI"
[2]Research and Production Corporation "Radiy"
[3]Centre for Safety Infrastructure-Oriented Research and Analysis
[1]V.Kharchenko@khai.edu
[2]research@radiy.com

Abstract

Challenges related to verification and validation (VV) of FPGA-based safety critical I&C systems (FICS) are analyzed. One of the mandatory techniques applied in process of VV and certification to requirements of IEC 61508 according with safety integrity level (SIL) is the fault insertion or injection testing (FIT). Specific features of FICS SIL-certification and FIT are described. Concept of FIT-ability, some theoretical issues and algorithm of the optimal FIT procedure taking into account different points and means of fault injection are suggested. The developed technique and tool VTP has been applied to verify modules of FPGA-based platform RadICS during SIL-certification.

1. Introduction

1.1. Motivation

FPGA technology more and more intensively is applied in safety critical domains, first of all, in instrumentation and control systems (I&C) of nuclear power plants (NPP), on-board aerospace systems and medical embedded equipment [1-3]. It caused by a few advantages of FPGA-based I&Cs (FICS) in comparing with SW-based ones implemented using microprocessors and microcontrollers with universal and fixed architecture. In particular, application of FPGA technology ensures more high reliability, safety and security, the best flexibility and maintainability.

On the other side, this technology causes a few specific risks which must be decreased to acceptable level. Besides, FICSs for critical application such as NPP I&Cs should meet to requirements of international and national regulatory bodies, corresponding standards, first of all IEC 61508 [4]. The key requirement relates to independent verification and validation (IVV). Usually the IVV of most sophisticated safety critical I&Cs (for example, reactor trip systems) is carried out by a team (company) which is organizationally and financially independent relatively a team developed and produced the system.

There are a lot of verification techniques applied during IVV process for FICSs based on documentation analysis, problem review, static analysis of VHDL code, testing and others. One of the mandatory techniques applied in process of certification to requirements of IEC 61508 according with safety integrity level (SIL) is the fault insertion or injection testing (FIT) [5]. The increasing of complexity of FPGA design and safety critical FICSs (the number of channels and versions on application diversity principle is a reason to research and develop FIT procedures taking into consideration the modern challenges.

1.2 Features of FIT technique application for SIL-certification of FICS

FIT is well-known technique used to verify different SW-, HW- and FPGA-based projects [5-7]. There are a lot of technique modifications, in particular, simulation- and prototype-based groups [6]. Verifiers inject faults into the components and FICS to evaluate test unit set completeness and quality, effectiveness of fault- or intrusion-tolerance and demonstrate actual level of dependability and safety. However, there are not detailed regulation requirements and SIL-oriented FIT techniques for FICSs. SIL-certification and verification of FICS, in particular, for NPP I&C, have a few specific features:

- existing of several level of FIT implementation (system, module, chip of FPGA, VHDL code); first

978-1-4799-2096-9/13/$31.00 ©2013 IEEE

three levels are more HW (physical) fault injection-oriented, forth one is design fault injection-oriented;

- FIT procedure for module level should be realized taking into account approved results of failure modes and effect criticality analysis (the results of FMECA technique or their modifications [8]);
- injection of HW faults and approving of injected faults detection must be demonstrated on the developed and produced module using a special tools.

Such features cause additional problems of FIT technique development and implementation taking into account cost of the sophisticated equipment and complexity of module design.

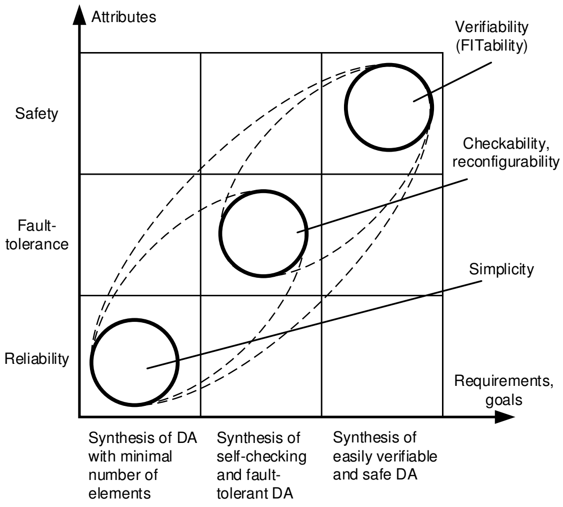
Goal of the paper is to formulate a general idea of FICS (and digital systems as a whole) ability to FIT called FIT-ability and to propose technique of optimal FIT taking into account existing a set of injection variants for HW physical faults and restrictions of injection for produced scheme.

The paper is structured by the following way. Second section is dedicated to discussion of concept FIT-ability in context of digital system evolution. Third one presents formal concepts of FIT process, optimization algorithm and example of FIT procedure development. Forth section describes case study and fifths one concludes discussion.

2. FIT and FIT-ability

2.1. Evolution of system abilities: FIT-ability stage

Let's analyze an evolution of main attributes related to I&C reliability and safety in context of FIT as one of the modern techniques of system verification.



Attributes
Verifiability (FITability)
Safety
Checkability, reconfigurability
Fault-tolerance
Simplicity
Reliability
Requirements, goals
Synthesis of DA with minimal number of elements
Synthesis of self-checking and fault-tolerant DA
Synthesis of easily verifiable and safe DA

Figure 1. The stage of the evolution attributes

Three main stages of the evolution may be selected (Figure 1):

- the first stage (1950-1960th years): synthesis of digital automata (DA) with minimal number of elements; the main requirements concerned simplifying and reliability assurance;
- the second stage (1970-1990th years): synthesis of self-checking DA and fault-tolerant systems; the main requirements concerned checkability and reconfigurability assurance;
- the third stage (2000-2010th years): synthesis of easily verifiable and safe DA; new additional requirement for safety critical domains is assurance of safety and demonstrability of the required level of safety on the development, validation and operation. In this case we can speak about verifiability as important attribute of I&C.

2.2. Concept of FIT-ability

As FIT is key and mandatory IVV technique, on the one side, and taking into account its complexity and some restrictions which are typical for safety important projects, on the other side, it's reasonably to suggest to introduce a concept of the ability of automata (I&C and FICS) to fulfillment of fault injection testing and to call it *FIT-ability* (a concept fitability is used in other, non IT areas and mean ability to fitting). Further we'll talk about prototype-based FIT-ability, i.e. ability to inject faults regarding to actual physical scheme (or code) and not to model of this system. FIT is a subattribute of verifiability and in turn consists of a few characteristics determining complexity of tools for FIT support, simplicity of fault injection and reinjection, etc. Metrics for FIT assessment are the number and complexity (time and cost) of fault injection and reinjection operations.

As stated above FICS has three levels for FIT (see Figure 2). Hence, for SIL-oriented process of FICS certification concept of FIT-ability may be specified as ability to fulfillment of fault injection testing according with FMEDA results on different level of system hierarchy: (SW, i.e. VHDL) FMEDA, (Chip) FMEDA, (Module) FMEDA, (Cabinet) FMEDA and (System) FMEDA.

3. Optimal FIT Procedure

3.1. Theoretical Issues

Let's describe a scheme S_{FIT} which is object of FIT procedure may be presented by a pair:

$$S_{FIT} = <G = \{A, B\}, T_{FMEDA} >, \quad (1)$$

where $G = \{A, B\}$ – structure graph of S consisting of a set of nodes (elements of scheme), $A = \{a_x\}$, and a set of edges $B = \{b_y\}$;

$T_{FMEDA}= \{f_i, m_i, e_i, d_i, c_i\}$ – a set (FMEDA table) consisting of subsets of faults f_i, modes m_i, effects e_i, diagnostic attributes d_i, defining possibility (detecting) of fault f_i, and criticality of fault c_i, $i = 1,\dots,F$. In fact, FMEDA table presents the list of symptoms which should be realized for the scheme verified. The table defines project-oriented profile of injected faults.

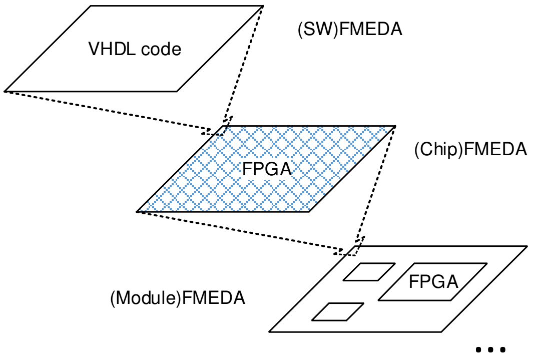


Figure 2. The levels of FMEDA and FIT procedure for FIC S

For FICS

$$FMEDA = (SW)FMEDA \cup (Chip)FMEDA \cup \cup (Module)FMEDA \cup (Cabinet)FMEDA \cup \cup (System)FMEDA. \quad (2)$$

Next task is determining of position (point of scheme) pf_i and means mf_i of injection for all faults f_i. In general pf_i and mf_i are sets $pf_i = \{pf_{ij}\}$, $mf_i = \{mf_{ik}\}$, $j = 1,\dots, npf_i$; $k = 1,\dots, nmf_i$, and

$$\exists i,v,\ i \neq v: pf_i \cap pf_v \neq \varnothing, mf_i \cap mf_v \neq \varnothing. \quad (3)$$

Full FIT covered space of f_i ($FFCSf_i$) will call a set receiving as a Cartesian product:

$$FFCSf_i = pf_i \text{ x } mf_i. \quad (4)$$

Full FIT covered space of scheme (FFCS) is an aggregation of all $FFCSf_i$:

$$FFCSS = \cup FFCSf_i, , i = 1,\dots,F. \quad (5)$$

A special FFCS table corresponds full FIT covered space of scheme. Trivial FIT covered space of f_i ($TFCS_i$) will call a set for which:

$$\forall pf_{ij}\ \exists!\, mf_{ij}, Card\ TFCS_i = npf_i;$$

$$TFCS = \cup TFCSf_i, TFCS_{i,} \subseteq FFCSf_i, \quad (6)$$
$$TFCS \subseteq FFCSf.$$

Implemented FIT covered space of scheme (IFCS) is a subset of $FFCS$, $IFCS \subseteq FFCS$ (and $TFCS \subseteq IFCS$) and should be developed taking into account a set of restrictions $FITR = \{r_z\}$ for fault injection on different levels of the systems. The following restrictions of physical fault injection into verified system (hardware module) including:

- r_1: element parameters are not changed under temperature and mechanical influences;
- r_2: fault injection for element $a_x \in A$ (in space of element a_x) does not cause failure or unacceptable parameter changing of other elements a_q ;
- r_3: any element $a_x \in A$ must be technologically acceptable for fault injection.

Hence,

$$IFCS = FITR \blacklozenge FFCS, \quad (7)$$

where ♦ - operation of the FFCS set filtration by the FITR set. IFCS is described by sets of *positions* $Ipf_i = \{Ipf_{ij}\}$ and means $Imf_i = \{Imf_{ik}\}$, $j = 1,\dots, Inpf_i$; $k = 1,\dots, Inmf_i$. It's understandable that $\forall Ipf_{ij} \subseteq pf_{ij}$, $\forall Imf_{ik} \subseteq mf_{ik.}$

3.2. Algorithm

To develop optimal FIT procedure according with analysis of S_{FIT} and T_{FMEDA} it's need to fulfill the following operations.

1. The receiving of sets $FFCSf_i$, FFCSS and corresponding tables (Tables 1). The feature of this stage is necessary of correct understanding and technological interpretation of FMEDA-based symptom.

Table 1. Table of FFCS

Faults, f_i	Attributes of fault injection	
	Points, pf_i	Means, mf_i
f_1	pf_1	mf_1
…	…	…
f_F	pf_F	mf_F

2. The building of IFCS table taking into account the restrictions set FITR (Table 2).

3. The finding of irredundant sets for IFCSs (irIFCS = {$irIFCS_h$}). Well-known algorithm of Boolean matrix coverage may be used for that. Initial IFCS may be rebuilt in more convenient way to solve the coverage task (Table 3) taking into account expression (3) describing possibility of application of the same points (and means) to inject different faults.

Table 2. Table of IFCS

Faults, f_i	Attributes of fault injection	
	Points, Ipf_i	Means, Imf_i
f_1	Ipf_1	Imf_1
…	…	…
f_F	Ipf_F	$I\ mf_F$

This transformed table is Boolean matrix, and its elements equal 1 or 0 depending on use of point Ipf_{ik} to inject fault f_i by corresponding means.

4. The choosing of the minimal implemented FIT covered space $IFCS_{min}$ according with criteria of optimum. Such criterion may be cost of f_i injection by use of corresponding position pf_i and means mf_i.

Table 3. Transformed IFCS table

Faults, f_i	Means, Imf_i	Points, Ipf_i						
		Ipf_{11}	…	Ipf_{1Inpf1}	…	Ipf_{F1}	…	Ipf_{FInpfF}
f_1	Imf_{11}							
	…							
	Imf_{1Inmf1}							
…								
f_F	Imf_{F1}							
	…							
	Imf_{FInmfF}							

3.3 An example

The suggested algorithm may be illustrated by example of the $IFCS_{min}$ development for the power supply module of the RadICS platform [9]. We'll illustrate below only two last operation of the algorithm.

For analyzed scheme the FMEDA table contains four symptoms for faults effecting lost of voltage: f_1 (PS.2,5v BANKS lost), f_2 (PS.2,5v VCCA lost), f_3 (PS.1,2v VCCINT lost), f_4 (PS.3,3v BANKS lost).

Every fault may be injected into one of the eleven points of the scheme (Ipf_i) by two means as "stuck off" (m_{i1}) or short circuit of pins "out&GND" (m_{i2}). Other variants were excluded taking into account the restrictions set (see transformed IFCS table, Table 4).

Table 4. Transformed IFCS table

Faults, f_i	Means, m_{ij}	Points, Ipf_i									
f_1 , PS.2,5v BANKS lost	m_{11}, stuck off	Ipf_1	Ipf_2	Ipf_3	Ipf_4	Ipf_5	Ipf_6	Ipf_7	Ipf_8	Ipf_9	Ipf_{10}
	m_{12}, out&GND	0	0	1	1	0	0	0	0	0	0
f_2 , PS.2,5v VCCA lost	m_{21}, stuck off	0	0	0	0	0	1	0	0	0	0
	m_{22}, out&GND	1	1	0	0	0	0	0	0	0	0
f_3 , PS.1,2v VCCINT lost	m_{31}, stuck off	0	0	0	0	1	0	0	0	1	0
	m_{32}, out&GND	0	0	0	0	0	0	1	0	0	0
f_4 , PS.3,3v BANKS lost	m_{41}, stuck off	0	0	0	0	0	0	0	0	0	1
	m_{42}, out&GND	0	0	0	0	0	0	0	1	0	0

According with known rule the coverage function is described by the following formula:

$$\Phi = (p3m11 \vee p4m11 \vee p6m12) \wedge (p1m21 \vee p2m21 \vee p5m22) \wedge (p9m31 \vee p7m32) \wedge (p10m41 \vee p8m42) = p3m11 \wedge p1m21 \wedge p9m31 \wedge p10m41 \vee p4m11 \wedge p1m21 \wedge p9m31\ p10m41 \vee p6m12 \vee p1m21 \wedge p9m31 \wedge p10m41 \vee \ldots \vee p6m12 \vee p5m22 \wedge p7m32 \wedge p8m42,$$

where $pimij \in \{0,1\}$ is logical value presented at the cell with row m_{ij} and column p_i.

In general we have 36 variants of the irIFCSs:

$$irIFCS = \{irIFCS_1=\{(p_3, m_{11}),(p_1, m_{21}),(p_9, m_{31}),(p_{10}, m_{41})\},\ldots, irIFCS_{36}=\{(p_6, m_{12}),(p_5, m_{22}),(p_7, m_{32}),(p_8, m_{42})\}\}.$$

Choosing of the IFCS$_{\text{min}}$ depends on injection costs for pairs (pf_i, m_{ij}). Let's assume that injection cost for all points is equal, and injection costs of "stuck off" (m_{i1}) more than "out&GND" (m_{i2}). In this case the best variant is the following

$$IFCS_{min} = \{(p_6, m_{12}),(p_5, m_{22}),(p_7, m_{32}),(p_8, m_{42})\}.$$

4. Implementation of FIT technique on SIL certification of FICS

The suggested technique has been applied to verify modules of FPGA-based platform RadICS during SIL-certification according with requirements of standards IEC61508 [9]. General process FIT-based verification is illustrated by Figure 3.

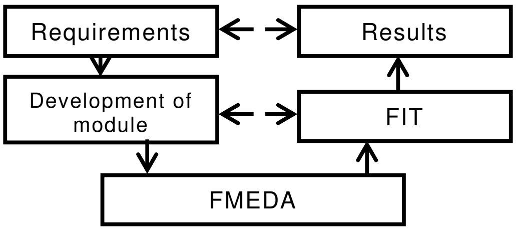


Figure 3. The FIT-based verification

FIT is carried out to check module response on injected fault on integration testing (IT) and system response on validation testing (VT). To fulfill FIT a special HW tool VTP (Validation Test Panel) was developed. The tool allows simultaneously injecting one or more faults, to set the fault type and indicate required data, check uncontrolled injection risks. VTP is a part of the IVV system integrating National Instruments modules and software tool LabView.

5. Conclusion

FIT-ability has became important safety related attribute for FPGA-based modules and critical I&C systems as allows to improve their demonstratability and verifiability. There a lot of FIT implementation variants and restrictions of fault injection. The suggested algorithm optimizes their selection according with cost-effective approach. One of the future steps based on the presented outcomes may be connected with development of the recommendations for improving FIT-ability FPGA-based modules and FICS as a whole, and development of the FIT-modifications for security assessment.

6. Reference

[1] V. Kharchenko, V. Sklyar (eds.). *FPGA-based NPP I&C Systems: Development and Safety Assessment*, RPC Radiy, National Aerospace University KhAI, SSTC on Nuclear and Radiation Safety, Kharkiv-Kirovograd, 2008.

[2] T. Huffmire, C. Irvine, Thuy D. Nguyen, T. Levin, R. Kastner, T. Sherwood. *Handbook of FPGA Design Security*, Springer, New York, 2010.

[3] V. Hahanov, E. Litvinova, O. Guz'. *Design and Testing of SoC.* Kharkiv National University of Radio Electronics, Kharkiv, 2009.

[4] M. Medoff, R. Faller. *Functional Safety - An IEC 61508 SIL 3 Compliant Development Process*, www.exida.com

[5] D. Cotroneo. *Innovative Technologies for Dependable OTS-Based Critical Systems: Challenges and Achievements of the CRITICAL STEP Project*, Springer, Milan, 2013.

[6] M. Hsueh, T. Tsai, R. Iyer. *Fault Injection Techniques and Tools*, IEEE Computer, vol. 30, no. 4, 1997, pp. 75-82.

[7] R. Leveugle. *Fault Injection in VHDL Descriptions and Emulations*, Proceedings of DFT'2000 Conference, October, 2000, pp. 414-419.

[8] E. Babeshko, V. Kharchenko, A. Gorbenko, *Applying F(I)MEA-Technique for SCADA-Based Industrial Control Systems Dependability Assessment and Ensuring*, Proceedings of the 3rd International Conference on Dependability of Computer Systems DepCoS, Szklarska Poreba, June, 26-28, 2008, pp. 309-315.

[9] A. Andrashov, V. Kharchenko, A. Siora, V. Sklyar, A. Volkoviy. *Certification of FPGA-based Safety Instrumentation and Control Platform in Accordance with IEC 61508*, Proceeding of the 1st International Workshop Critical Infrastructure Safety and Security CrISS-DESSERT, vol. 1. Kirovograd, Ukraine, May, 11-13 2011, 2011. pp. 148-152.