IEEE

PROCEEDINGS of
2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies

DESSERT'2018

Ukraine, Kyiv
May 24-27, 2018

ORGANIZED BY

IEEE Ukraine Section
IEEE Ukraine Section SP/AES Societies Joint Chapter
IEEE Ukraine Section (Kyiv) ED/MTT/CPMT/COM/SSC Societies Joint Chapter
IEEE Ukraine Section (Kharkiv) SP/AP/C/EMC/Com Societies Joint Chapter
IEEE Ukraine Section IM/CIS Societies Joint Chapter
National Aerospace University n. a. N. E. Zhukovsky "KhAI", Kharkiv, Ukraine
Banking University, Kyiv, Ukraine
National Aviation University, Kyiv, Ukraine

EXCLUSIVE PARTNERS

Research and Production Corporation Radiy, Ukraine
National Bank of Ukraine

IEEE Ukraine Section
National Aerospace University n. a. N. E. Zhukovsky "KhAI", Kharkiv, Ukraine
Banking University, Kyiv, Ukraine
National Aviation University, Kyiv, Ukraine
IEEE Ukraine Section SP/AES Societies Joint Chapter
IEEE Ukraine Section (Kyiv) ED/MTT/CPMT/COM/SSC Societies Joint Chapter
IEEE Ukraine Section (Kharkiv) SP/AP/C/EMC/Com Societies Joint Chapter
IEEE Ukraine Section IM/CIS Societies Joint Chapter

Conference Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies

DESSERT'2018

Ukraine, Kyiv, May 24-27, 2018

Additional copies may be ordered from:

IEEE Operations Center
445 Hoes Lane, P.O. Box 1331,
Piscataway, NJ 08855-1331 USA

DESSERT'2018 Organizing Committee
National Aerospace University n. a.
N. E. Zhukovsky "KhAI",
Computer Systems, Networks and
Cybersecurity Department
Chkalov str., 17, Kharkiv, 61070, Ukraine
Phone: +38 (095) 564 76 69
e-mail: dessert@csn.khai.edu

EEE Catalog number:
CFP18P47-USB
ISBN 978-1-5386-5902-1

For paper:
EEE Catalog number:
CFP18P47-ART
978-1-5386-5903-8

Table of Contents

Influence of Diagnostics Errors on Safety: Indicators and Requirements

Yuriy Ponochovniy [1], Eugen Bulba [2], Alina Yanko [3], Egor Hozbenko [4]
[1,3] Poltava National Technical University, Poltava, Ukraine, yuriy.ponch@gmail.com, al9_yanko@ukr.net, http://fitts.pntu.edu.ua/ua/kafedry/komp-iuterna-inzheneriia
[2,4] Research and Production Company Radiy, Kropyvnytskyi, Ukraine, evhenb@gmail.com, egorgozbenko@ukr.net, http://radiy.com

***Abstract*: In article questions of intersection of indices of technical diagnostics and the functional safety are considered. The relevant standards on diagnostics (IEC 60706-5-2007) and the functional safety (IEC 61508-4:2010) determining indices of a completeness and reliability of diagnosing, a share of safe failures and spanning by diagnostics are defined. Requirements to indices of the functional safety for achievement of the necessary level of a completeness of safety of electronic systems are selected. Influence of errors of system of diagnosing on indices of the functional safety is considered that allows to specify their assessment before carrying out evaluation tests.**

Keywords: Diagnostic testing, Diagnosis correctness, Test coverage, Safe failure fraction, Diagnostic coverage

I. INTRODUCTION

Today, the application of functionally safe systems is conditioned not only by the requirements of regulatory authorities but also by a large number of bitter examples of catastrophic consequences of failures. In the field of the standardization of functional safety, industry standards for automotive, railroad and aerospace industries, nuclear power industry and electronic programmable devices have been developed [1-3]. These standards determine the order for devices and systems certification to a certain level of safety integrity. Such certification is carried out by responsible organizations, for example, Exida [4]. During certification process, the evaluation of the functional safety parameters of the object (system) is performed. It is worth noting that the certification procedures are laborious and expensive.

The theory of technical diagnostic is highly developed in the post-USSR countries. The issues of assessing the parameters and improving the quality of technical diagnostic are relevant and covered in the works [5,6]. Standard [7] define the composition of the parameters of technical diagnostic; models, and methods for their evaluation are considered in [8,9]. For a number of electronic programmable systems, the parameters of technical diagnostic can be determined by the internal expert authority/employee without the involvement of external auditors. The purpose of this work is to research the influence of the parameters of technical diagnostic on the indicators of functional safety.

II. PARAMETERS OF DIAGNOSTIC TESTING

The basic definitions in the field of technical diagnostic are standardized in [7]. A later international standard IEC60706-5 [10] regulates diagnostic tests. Technical diagnostic is defined as process of determining the technical state of an object.

In technical diagnostic, four combinations of operable and inoperative states of the object of diagnosis and the diagnostic and monitoring system are considered.

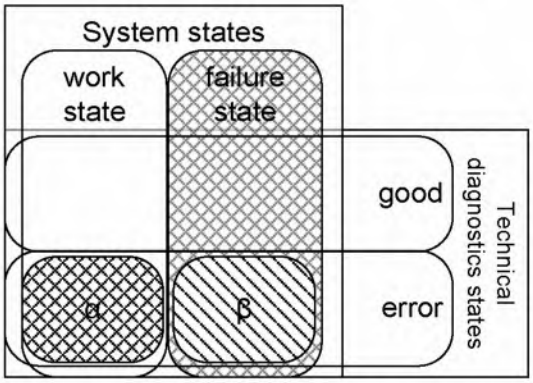


Figure 1. Intersections of the sets of state spaces of technical diagnoses

The errors of the diagnostic system are divided into errors of the first and second type. Errors of the third type also appear in the works by [11,12], but here they are not considered.

An error of the first type (manufacturer's risk, α) is the probability that the measured parameter is within acceptable range when obtaining a result of parameter over-range.

An error of the second type (customer risk, β) is the probability that the measured parameter is out of range when obtaining a result that it is within acceptable range.

In the standard [10] there is a definition: false alarm - the indication of failure which, after carrying out failure finding activities, is not found; and false alarm rate - the

percentage of false alarms in the total number of failure indications.

Among the listed in the standards [7,10] indicators of technical diagnostic and monitoring of technical condition, we were interested in two: the diagnosis correctness and the test coverage.

Diagnosis correctness - proportion of faults of an item that can be correctly diagnosed under given conditions.

Test coverage - ratio of the number of faulty functions actually capable of diagnosis by the given test instruction to the total number of functions

The early standard [7] does not define methods and models for calculating diagnostic indicators. In different studies, different approaches to definition both diagnosis correctness and test coverage are used.

In the work [12], test coverage is considered in a "broad" sense. It is defined as the product of:

- indicator of diagnostic model compliance to the object D_{CONF},
- the diagnosis correctness D_{CORR},
- and the instrumental validity D_I.

The diagnosis correctness is determined as the ratio of number *m* of the object measured diagnostic parameters of to the number *n* of parameters of the diagnostic model [13].

$$T_C = D_{CONF} \cdot D_{CORR} \cdot D_I; \quad D_{CORR} = m/n. \quad (1)$$

In work [8], the test coverage is defined as the probability of correctly diagnosing the operable and inoperative states of an object or system. (It should be noted here that in [12] such test coverage is called instrumental validity).

$$T_C = 1 - P_{DiagnError} = 1 - \left(P_\alpha + P_\beta\right). \quad (2)$$

To determine the correctness of the diagnosis in [12,14] it is proposed to use the approach based on reliability indicators:

$$Dc = \sum_{i=1}^{n} \lambda_i \Big/ \sum_{k=1}^{m} \lambda_k, \quad (3)$$

where *i* defines the sum of the intensity of the malfunctions detected by the test (diagnostic system); *k* defines the sum of the intensities of all possible malfunctions (*n* and *m* are the numbers of detectable and all possible malfunctions, respectively).

If it is difficult to determine the values of the failure rates of elements for modern diagnostic objects, it is recommended to use an estimate of the upper limit of possible values of the completeness of the test. It is defined as the percentage of malfunctions which are tested by the formula:

$$D_{corr}^{\uparrow} = \left[\left(G - G1\right)/G\right] \cdot 100\%, \quad (4)$$

where G is the number of all admissible faults, G1 is the number of non-verifiable faults.

According to the standard the [10] diagnosis correctness (Dc) and the test coverage (Tc) are defined as:

$$Dc = \frac{A' + B' + C' + D'}{A + B + C + D} \le 1, \quad (5)$$

$$Tc = \frac{A'' + B'' + C'' + D''}{A + B + C + D} \le 1, \quad (6)$$

where [A'; B'; C'; D'] - tests leading to a correct diagnosis for on-line tests, off-line tests, external tests and maintenance tests,

[A''; B''; C''; D''] - tests actually provided for online tests, off-line tests, external tests and maintenance tests,

[A; B; C; D] - tests during operation for online tests, offline tests, external tests and maintenance tests.

Thus, the composition of the calculation formulas is influenced by the availability of certain input parameters for the researchers (the number of malfunctions, the probability of detection, the failure rates).

III. FUNCTIONAL SAFETY PARAMETERS

According to [15], to assess functional safety, set of system failures are divided into subsets of safe (MS) and dangerous (MD). Usage of monitoring tools, real-time testing and diagnostics allows to detect failures, which causes the definition of four failures subsets:

- SD: safe detected,
- SU: safe undetected,
- DD: dangerous detected,
- DU: dangerous undetected,

Each failures subset is characterized by the corresponding parameter - failure rate. As in reliability theory, the failure rate is defined as:

$$\lambda(t) = \frac{-R'(t)}{R(t)}. \quad (7)$$

In the most common case, with an exponential time distribution between failures, the failure rate is a stationary value. Then the dependencies are valid:

$$\lambda_S = \lambda_{SD} + \lambda_{SU}; \; \lambda_D = \lambda_{DD} + \lambda_{DU}. \quad (8)$$

The following figure shows how four failures subsets are formed.

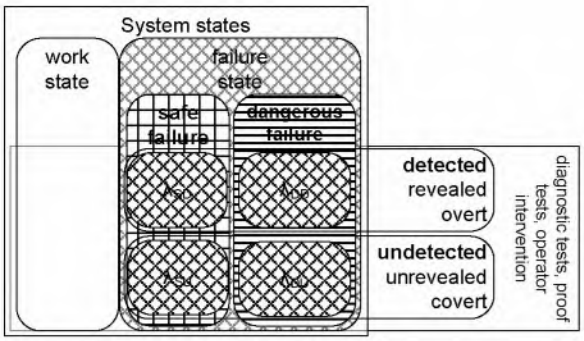


Figure 2. Subsets of failures that are analyzed in assessing functional safety

In the standard IEC61508 [15] the greatest interest (to the issue of link with the parameters of technical diagnosis) is caused by two parameters: the fraction of safe failures and the coverage of diagnostics. These indicators are not resultant, but are present in the check-list of compliance to a definite safety integrity level.

In the standard IEC61508 [15] two indicators are of greatest interest (from view-point of relations with parameters of technical diagnostics): safe failures fraction and diagnostic coverage. These indicators are not resultant, but in a number of cases are present in the check-list of compliance to a certain safety integrity level (SIL).

Safe failure fraction (SFF) - property of a safety-related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. When the failure rates are based on constant failure rates the equation can be simplified to:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_D} = 1 - \frac{\sum \lambda_{DU}}{\sum \lambda_S + \sum \lambda_D} \quad (9)$$

Diagnostic coverage (DC) – a fraction of dangerous failures detected by automatic on-line diagnostic tests. The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} \quad (10)$$

Thus, in the area of functional safety, the SFF and DC indicators refine the diagnostic characteristics for a subset of dangerous failures.

IV. INFLUENCE OF DIAGNOSTICS ERRORS ON FUNCTIONAL SAFETY FAULTS SPACES

Studying the standard of functional safety IEC61508, the authors came to the conclusion that the proposed models consider a diagnostic system with an error probability close to unity. (The definition of a diagnostic error is not mentioned in the text of the standard). But at the same time, a safe failure is considered as leading to a false safety function. Thus, it was concluded that errors of the first type can be considered as safe failures. Errors of the second type expand the set of safe and dangerous undetected failures.

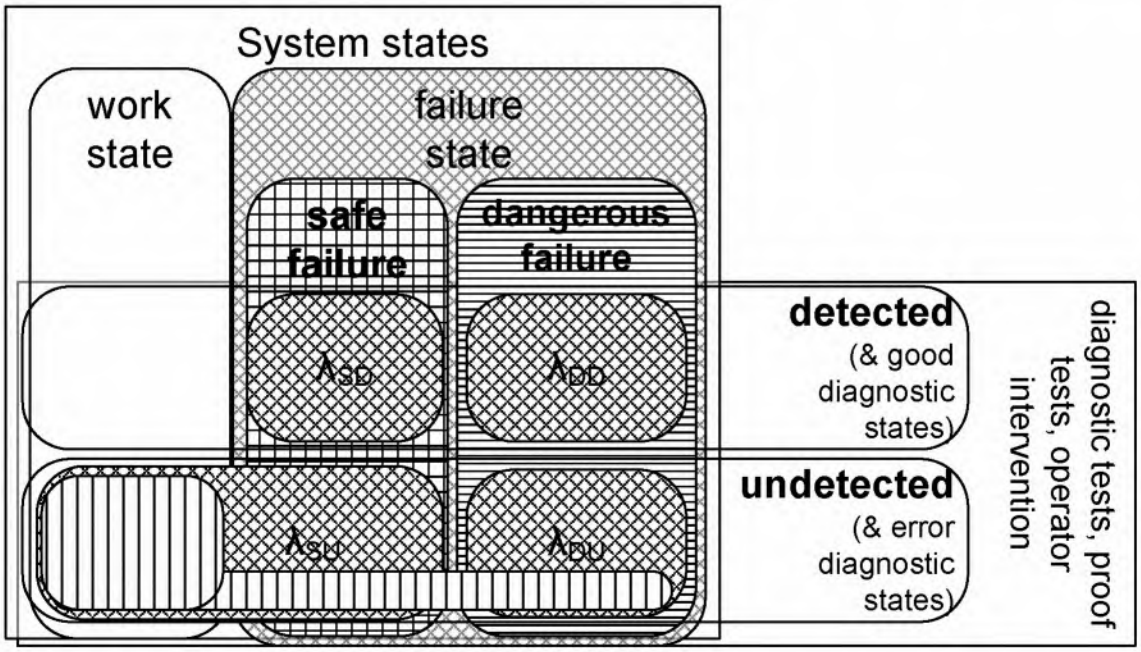


Figure 3. Extension of a undetectable failures subset when taking into account the diagnostic errors of the second type

Thus, in the functional safety designation space, the diagnosis correctness and test coverage can be defined as:

$$Tc = \frac{\lambda_{SD} + \lambda_{DD}}{\lambda_S + \lambda_D} = SFF - \frac{\lambda_{SU}}{\lambda_S + \lambda_D} \quad (11)$$

$$D_C = 1 - P_{DiagnError} = e^{-\lambda'_{SU} \cdot t} + e^{-\lambda'_{DU} \cdot t} \quad (12)$$

V. CASE FOR FPGA-BASED SAFETY CONTROLLER RADICS

The FPGA-based Safety Controller (FSC) RadICS is essentially a safety PLC, except that its internal logic is performed by FPGAs instead of microprocessors. The FSC is composed of a logic module (LM) and a number of varied I/O modules contained within a chassis, just like a general-purpose safety PLC [16].

Figure 4 shows the basic hardware arrangement of the FSC, showing 2 dedicated slots for Logic Modules (LM) and 14 available slots for any mixture of I/O modules.

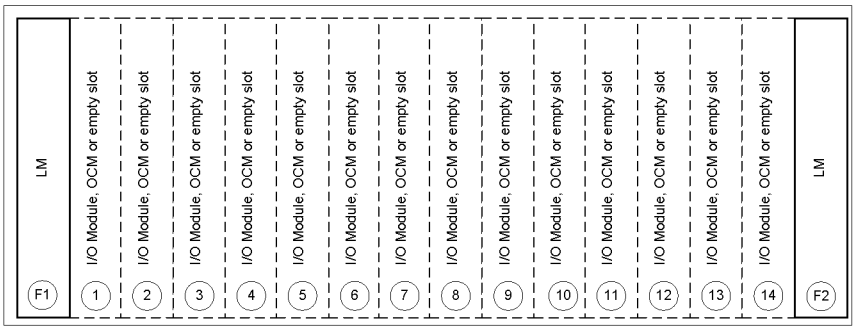
Techniques for safety integrity and functional safety assurance that are used in FSC can be divided into 3 main groups:

1) Hardware Self-diagnostics (HW SD);

2) Interfaces and Data Transmission Self-diagnostics (IF SD);

3) FPGA Electronic Designs Self-diagnostics (ED SD).

These tests are performed during short diagnostic intervals (t <300 ms) during platform operation.



Modules:

LM	Logic
AIM	Analog Inputs
DIM	Digital Discrete Inputs
DOM	Digital Discrete Outputs
AIFM	Analog Input Flux
AOM	Analog Outputs
OCM	Optical Communication
RIM	RTD Inputs
TIM	Thermocouple Inputs
WAIM	Wide Range Analog Inputs

Figure 4. FPGA-based Safety Controller, Chassis Configuration

In low demand mode applications, credit can be taken for proof tests. The DUPT (dangerous undetected after proof test) failure rates take into account the effectiveness of a thorough proof test in addition to the self-diagnostics. In this context, a thorough proof test is one in which all safety-critical inputs are caused to evolve through all critical values which permit the tester to confirm that the SIS is working correctly and completely. The DUPT failure rates for each module or channel are also provided in the Table I.

The process industry usually performs proof tests at intervals of 1 to 3 years. For the example provided, the valves and associated I/O are tested once per year because the NFPA (National Fire Prevention Association) standard NFPA 85 requires valves to be tested every 12 months. The FSC and the sensors and associated I/O on the other hand are tested once per 3 years in order to confirm the FSC requirements.

For low demand mode, the expected demand interval is at least one year, and the proof-test period is at most ½ of the expected demand period. This means that the proof test must be performed at least twice within the expected interval between demands on the FSC.

The Proof Test Coverage (PTC) can be calculated using the formula:

$$PTC = 1 - \lambda_{DUPT} / \lambda_{DU} \quad (13)$$

The analysis for FSC proof-testing at 3 years (every 36 months) intervals arises from the FSC: these results confirm the FSC requirements are met.

TABLE I. FSC FAILURE RATES FOR CASE (ALTITUDE = 3000M)

Device	N	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	λ_{TOT}	$\lambda_{DD}+\lambda_{AD}$	λ_{DUPT}
LM Common	1	45837	77	45563	28.3		47022	3.6
AIM Common	1	2077	8.9	2052	9.3		5352	8.9
AIM AI	3	311	3.1	359	4.2		914	3.8
DOM Common	1	2084	10.5	2043	9.3		5407	8.9
DOM DO	2	65	0.7	57.4	2.7		393	0.6
λ totals for the FSC for this SIF		50374	100	50074	53.8	100602	59088	25.8

In the Table I λ_{AD} – the rate of failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.

The corresponding limits for Safety Integrity Level (SIL) 2 and SIL 3 that apply to a complete SIF (including sensors, the FSC and final elements) are SFF > 90% for SIL2 and SFF > 99% for SIL3.

As a result of the certification, the FSC platform RadICS received an SFF rating of 99.9%, which corresponds to SIL3. The value of Proof Test Coverage was 52%

CONCLUSIONS

The article considers two approaches to the definition and evaluation of diagnostic parameters. Standards have been singled out that regulate the determinations of diagnosis correctness, test coverage, safe failure fraction, diagnostic coverage. Models for estimating these parameters are analyzed and intersections of state spaces and failures subsets are identified.

The case for FPGA-based safety controller RadICS is considered. For platform modules, 3 types of Self-diagnostics, as well as Proof Test, are performed. According to the conducted certification evaluations for the Proof Test period of 3 years (1 year for valve testing), the platform has SFF = 99.9%, which corresponds to SIL3.

The direction of future research is the estimation of the diagnostic errors influence in case of the non-exponential distribution of failures.

REFERENCES

[1] ISO26262-1:2011, "ISO 26262-1:2011 - Road vehicles -- Functional safety -- Part 1: Vocabulary", *Iso.org*, 2018. [Online]. Available: https://www.iso.org/standard/43464.html. [Accessed: 03- Mar- 2018].

[2] CENELEC - EN 50126-1, "Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1", *Standards.globalspec.com*, 2018. [Online]. Available: https://standards.globalspec.com/std/10262901/cenelec-en-50126-1. [Accessed: 03- Mar- 2018].

[3] IEC 61513:2011, "Nuclear power plants - Instrumentation and control important to safety - General requirements for systems", *Webstore.iec.ch*, 2018. [Online]. Available: https://webstore.iec.ch/publication/5532. [Accessed: 03- Mar- 2018].

[4] Exida - Functional Safety Services, ICS Cybersecurity, Alarm Management, IEC 61508 Certification", *Exida.com*, 2018. [Online]. Available: http://www.exida.com/. [Accessed: 03- Mar- 2018].

[5] S. Uvaysov, et al., "Definition of a Set of Diagnostic Features at a Given Depth and Completeness of Testing Electronic", *DAAAM International Scientific Book 2014*, pp. 625-632, 2014.

[6] V. Kharchenko et al. "Fundamentals of Digital Systems Diagnostics", *National. aerospace Un-t M. E. Zhukovsky "KhAI"*, 2004. 664 p. (in Ukrainian)

[7] GOST 20911-89. Technical diagnostics. Terms and definitions. *Moscow: Standardinform*, 1989. 11 p. (in Russian)

[8] X. Tan, J. Qiu, G. Liu, K. Lv, S. Yang and C. Wang, "A novel approach of testability modeling and analysis for PHM systems based on failure evolution mechanism", *Chinese Journal of Aeronautics*, vol. 26, no. 3, pp. 766-776, 2013.

[9] Y. Zonghao, H. Huafeng, L. Tianmei, X. Congqi and Y. Zongxian, "Expected Bayesian tracking of testability growth under entropy loss function," *2017 Prognostics and System Health Management Conference (PHM-Harbin)*, Harbin, 2017, pp. 1-6.

[10] IEC 60706-5:2007, "Maintainability of equipment - Part 5: Testability and diagnostic testing", *Webstore.iec.ch*, 2018. [Online]. Available: https://webstore.iec.ch/publication/3015. [Accessed: 03- Mar- 2018].

[11] A. Drozd et al., "On-line testing of the safe instrumentation and control systems", *National. aerospace Un-t M. E. Zhukovsky "KhAI"*, 2012. 614 p. (in Russian)

[12] V. Kharchenko, V. Sklyar, A. Kh. Al-Tarazi. "State and event models of fault-tolerant information-control systems with their influence on safety" *Radiotechnical and computer systems*. Vol.2 2004. P. 67-74. (in Russian)

[13] G. Wang and J. Sun, "BIST-Based Method for Diagnosing Multiple Faulty CLBs in FPGAs", *Applied Mechanics and Materials*, vol. 643, pp. 243-248, 2014.

[14] M. Drozd, A. Drozd, "Safety-Related Instrumentation and Control Systems and a Problem of the Hidden Faults" In *10th International Conference on Digital Technologies,* Zhilina, Slovak Republic, 9 – 11 July, 2014, P. 137 – 140

[15] IEC61508-4:2010 "Functional safety of electrical/electronic/programmable electronic safety related systems. Definitions and abbreviations", *Thenbs.com*, 2018. [Online]. Available: https://www.thenbs.com/PublicationIndex/documents/details?Pub=BSI&DocID=313114. [Accessed: 03- Mar- 2018].

[16] D7.24-FSC(P3)-FMEDA-V6R0. Exida FMEDA Report of Project: Radiy FPGA-based Safety Controller (FSC), 2018, 69 p.