State of the art and development prospects of functional safety norms and standards

Alexander F. Kolchin, *Korporativnie elektronnie sistemy, Russia, Moscow*
Oleg S. Yakimov, *KVF Interstandart, Russia, Moscow*

Abstract. Aim. *Familiarizing the readers with the state of the art and development prospects of functional safety norms and standards in the Russian Federation. As the safety of any product, service or process is its second most important characteristic after the function, safety-related systems (SRSs) are widely used in order to ensure the safety of industrial, transportation, energy, communication and critical facilities, buildings and structures, urban infrastructure, as well as machines, equipment and vehicles. Unfortunately, since 1980's the technologies used in the development of the SRSs have not gained full traction in Russia. As the result, a conservative approach is in use that often involves excessive requirements, which increases the cost of the developed safety systems but usually does not guarantee compliance with the requirements. Currently, functional safety (FS) is recognized globally as the primary SRSs characteristic, that indicates the probability of successful performance by the system of the safety function(s) under the given conditions within the given time period.* **Methods.** *Globally, the implementation, further development and practical application of the FS method is based on the development and application of a large number of regulatory documents at the international, regional and national levels, that help organize and perform activities related to the assessment and FS requirements compliance confirmation for a wide range of SRSs. In order to ensure methodological support and coordination of the activities aimed at the development of FS-related regulatory framework in the Russian Federation in accordance with the national standard GOST R 1.1-2013 Standardization in the Russian Federation. Technical committees for standardization. Rules of organization and function, the technical committee for standardization TK 058 Functional Safety has been established, is actively working and has so far developed around 50 FS-related standards. The TK 058 standardization activities are based on the provisions of the Federal Law dated June 29, 2015 no. 162-FZ On standardization in the Russian Federation.* **Conclusions.** *As in the Russian Federation a certain FS-related regulatory framework has already been established, while the market shows demand for services of FS requirements compliance evaluation, the main task for today is to develop, using national and international requirements, organizational support, regulatory and guidance documentation that would create a fully-fledged infrastructure that implements the national institution of FS requirements compliance verification. That will ensure not only a radical reduction of the risk of disasters and accidents, but also significantly increase the competitiveness of Russian products in the internal and foreign markets.*

Keywords: *functional safety, regulatory framework, standardization, safety integrity level, certification, compliance evaluation*

For citation: Kolchin AF, Yakimov OS. State of the art and development prospects of functional safety norms and standards. Dependability 2017;3: p. 58-62. DOI: 10.21683/1729-2646-2017-17-3- 58-62.

Introduction

Everything that people create to meet their needs is essentially DANGEROUS (for people and for the environment). Therefore, creating any object should include identification and analysis of the hazards associated with that object. Thus, along with ensuring the availability of required functions for the created object, one must ensure the correct safe functioning (behavior) of that object, taking into account the interrelationships of the object's various systems with each other and the environment at all life cycle stages of that object.

For that reason, the safety of any product, service or process is its second most important characteristic after the function.

Safety-related systems (SRSs) are widely used in order to ensure the safety of industrial, transportation, energy, communication and critical facilities, buildings and structures, urban infrastructure, as well as machines, equipment and vehicles.

Unfortunately, since 1980's the technologies used in the development of the SRSs have not gained full traction in Russia. Their main shortcomings are:

1. Domestic developers and manufacturers of the SRSs, design and construction organizations, with rare exceptions, prefer to use old and obsolete regulatory documents based on prescriptive approach, even though compliance with the requirements of these documents does not guarantee the systems' performance and therefore does not guarantee the safety of the facility in which these systems are installed.

2. The SBSs and their subsystems are seen as autonomous independent production units (thing in itself), and their hazard/safety is assessed without taking into account the interrelationships of their components with each other and the environment.

As a result, a conservative approach is in use that often involves excessive requirements, which increases the cost of the developed safety systems, but usually does not guarantee compliance with the requirements.

Currently, functional safety (FS) is recognized globally as the primary STS characteristic, that indicates the probability of successful performance by the system of the safety function(s) under the given conditions within the given time period.

The FS method presented in the set of standards GOST R IEC 61508:

1. Uses a single (industry-independent) system integrated process approach and is aimed at identifying, preventing and mitigating the consequences of all safe failures, detected hazards, as well as reasonably predictable hazards and rare hazards that can lead to catastrophic consequences in complex technical systems.

2. Introduces a single measure of safety assessment, i.e. safety integrity level (SIL), which is presented and evaluated in terms of unacceptable risk of harm to people, property and the environment. The FS method implies a regular iterative process of hazard and risk analysis, an overall risk assessment and risk reduction measures that are implemented at all stages of the lifecycle of the SBSs. It also prescribes the actions of all individuals who can influence safety at these stages.

3. Is actively used in industrialized countries all around the world. Its application is regulated by more than 200 international, regional and interstate standards in various industries.

Globally, further development and practical application of the FS method is based on the development and application of a large number of regulatory documents at the international, regional and national levels that help to organize and perform activities related to the assessment and FS requirements compliance confirmation for a wide range of SRSs.

Although a number of Russian researchers have been dealing with FS problems for more than 20 years, a wide range of engineering and technical specialists became acquainted with the practical application of the FS method after the well-known works by David J. Smith and Kenneth J.L. Simpson [1, 2] were published in the Russian Federation and the first edition of the basic FS standard GOST R IEC 61508-2007 Functional safety of electrical, electronic, programmable electronic safety-related systems. Parts 1-7 were released in 2007.

In order to ensure methodological support and coordination of the activities aimed at the development of FS-related regulatory framework in the Russian Federation in accordance with the national standard GOST R 1.1-2013 Standardization in the Russian Federation. Technical committees for standardization. Rules of organization and function, the Technical Committee (TC) for Standardization TK 058 Functional Safety has been established and later restructured. In addition, several other related national technical committees for standardization of leading industries are also presently participating in the establishment of a national regulatory framework in the field of FS.

The TK 058 standardization activities are based on the provisions of the Federal Law dated June 29, 2015 no. 162-FZ On standardization in the Russian Federation.

The participation in TK 058 is voluntary.

The TC was established to enable cooperation among concerned organizations and authorities when performing national, interstate and international standardization activities in the field of FS.

The main goals of the TC in the field of FS standardization are:

- Developing annual national standardization programs and overseeing the implementation of these programs;
- Considering application of international and regional standards at the national and interstate level proposals;
- Carrying out scientific and technical, legal and regulatory examination of national and interstate standard projects and existing standards change projects and submitting them for approval to federal executive authority in standardization.

The results of this activities achieved over the past 10 years are briefly reviewed below.

The Russian standards in the field of FS

The focus of the TK 058 was on preparing the second edition of the basic standard IEC 61508-2010, as well as baseline FS standards for various industries. As a result, a set of standards GOST R IEC 61508-2010 [3-9] was established in 2012.

At the moment, the IEC 61511 [10-12] set of standards is actively used at a number of petrochemical, gas and electrical power enterprises that use safety instrumented systems to ensure the safety of various industrial processes.

Several international standards were introduced directly for the construction industry and national FS standards [13–19] were developed on the basis of IEC 61508 [13-19]. A number of corporate standards for construction industry have already been developed based on these regulatory documents.

A lot of attention in the Russian Federation is paid to the implementation of the FS method in railway transportation. A fairly large number of corporate standards for maintaining the guaranteed safety and reliability of the transportation process in JSC RZD have been developed and are now in use in the company. There are a large number of national and interstate FS standards in place in the railway industry, some of which are presented in [20-23].

In the nuclear power plant engineering, several standards concerning monitoring and control systems for the industry's various products have been developed, that comply with FS requirements [24–32].

The problems of FS of machines and mechanisms FS problems are considered in regulatory documents [33-36].

The implementation of the FS method for road vehicles control systems is presented in [37-47].

The general principles for the implementation of the IEC 61508 series requirements for safety-related data communication, including possible data communication failures, recovery measures and considerations related to data integrity in industrial communication networks can be found in [48-53].

Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions are presented in [54, 55].

FS requirements for programmable controllers are considered in [56].

At present, 4 more FS standards, including the 2-nd edition of IEC 61511-2016, have been developed and are awaiting approval.

From standardization to compliance assessment

Today it is practically impossible to export a complex technical system or its components without a confirmed safety integrity level compliance assessment.

Almost any complex systems delivered in the Russian Federation are marked with this characteristic that explicitly describes their safety.

Therefore, in most economically developed countries compliance confirmation (certification) agencies with corresponding institutions (testing laboratories/centers) providing measurements, tests, requirements compliance assessment calculations, are working to confirm FS requirements compliance of complex equipment, industrial facilities, systems and their components.

There is no national institution of FS requirements compliance verification in Russia yet, which not only radically increases the risk of disasters and accidents, but also significantly reduces the competitiveness of Russian products in the internal and foreign markets. Meanwhile, there are all the necessary conditions for the creation of such institution. A FS-related regulatory framework has already been established and is quite relevant, while the market shows demand for services of FS requirements compliance evaluation.

Therefore, the main task for today is to develop, using national and international requirements, organizational support, regulatory and guidance documentation that would create a fully-fledged infrastructure in the Russian Federation that implements the national institution of FS requirements compliance verification.

In March 2016 the Voluntary Certification System in the Field of Functional Safety (registration number ROSS RU.31461.04IDD0) was registered in the unified register of voluntary certification systems of the Federal Agency on Technical Regulation and Metrology. It certifies safety-related systems (SRSs), their components, related products, functional safety management systems of organizations and/or subdivisions that develop, produce and use SRSs: hazard and risk analysis, design, manufacture, installation, putting into operation, maintenance and repair, modernization, decommissioning of SRSs, safety-related systems development, manufacture and application tools. The FS certification authority is also to be accredited by the National Voluntary Certification System of the Russian Federation.

References

1. Smith DJ, Simpson KGL. Functional safety. A straightforward guide to applying IEC 61508 and related standards. Moscow: Tekhnologii; 2004.

2. Smith DJ. Reliability, maintainability and risk. Practical methods for engineers including reliability centered maintenance and safety-related systems. Moscow: Gruppa IDT; 2007.

3. GOST R IEC 61508-1-2012 Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements

4. GOST R IEC 61508-2-2012 Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2. Requirements for systems

5. GOST R IEC 61508-3-2012 Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3. Software requirements

6. GOST R IEC 61508-4-2012 Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 4. Terms and definitions

7. GOST R IEC 61508-5-2012 Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 5. Examples of methods for the determination of safety integrity levels

8. GOST R IEC 61508-6-2012 Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

9. GOST R IEC 61508-7-2012 Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 7. Techniques and measures

10. GOST R IEC 61511-1-2011 Functional safety. Safety instrumented systems for the industrial processes. Part 1. Terms, definitions and technical requirements

11. GOST R IEC 61511-2-2011 Functional safety. Safety instrumented systems for the industrial processes. Part 2. Guidelines for the application of IEC 61511-1

12. GOST R IEC 61511-3-2011 Functional safety. Safety instrumented systems for the industrial processes. Part 3. Guidelines for the determination of the required safety integrity levels

13. GOST R ISO/IEC 14762-2013 Information technology – Functional safety requirements for home and building electronic systems (HBES)

14. GOST R 53195.1-2008 Functional safety of building/erection safety-related systems. Part 1. General

15. GOST R 53195.2-2008 Functional safety of building/erection safety-related systems. Part 2. General requirements

16. GOST R 53195.3-2015 Functional safety of building/erection safety-related systems. Part 3. Requirements for systems

17. GOST R 53195.4-2010 Functional safety of building/erection safety-related systems. Part 4. Software requirements

18. GOST R 53195.5-2010 Functional safety of building/erection safety-related systems. Part 5. Techniques and measures on risk reduction, estimation methods

19. GOST R EN 50491-4-1-2014 General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 4-1: General functional safety requirements for products intended to be integrated in Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)

20. GOST R 55980-2014 Risk management on railway transport. Hazardous events classification

21. GOST 33432-2015 Functional safety. Policy and programme of safety provision. Safety proof of the railway objects

22. GOST 33433-2015 Functional safety. Functional safety. Risk management on railway transport

23. GOST R IEC 62279-2016 Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems

24. GOST R IEC 60880-2010 Nuclear power plants. Instrumentation and control systems important for safety. Software aspects for computer-based systems performing category A functions

25. GOST R IEC 62138-2010 Nuclear power plants. Instrumentation and control systems important for safety. Software aspects for computer-based systems performing category B or C functions

26. GOST R IEC 60987-2011 Nuclear power plants. Instrumentation and control systems important to safety. Hardware design requirements for computer-based systems

27. GOST R IEC 61513-2011 Nuclear power plants. Instrumentation and control important to safety. General requirements for systems

28. GOST R IEC 61225-2011 Nuclear power plants. Instrumentation and control systems important for safety. Requirements for electrical supplies

29. GOST R IEC 61226-2011 Nuclear power plants. Instrumentation and control systems important for safety. Classification of instrumentation and control functions

30. GOST R IEC 60709-2011 Nuclear power plants. Instrumentation and control systems important for safety. Separation

31. GOST R IEC 62340-2011 Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure

32. GOST R IEC 61500-2012 Nuclear power plants. Instrumentation and control important to safety. Data communication in systems performing category A functions

33. GOST R IEC 62061-2013 Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems

34. GOST R IEC 61800-5-2-2015 Adjustable speed electrical power drive systems. Part 5-2. Functional safety requirements

35. GOST R 60.1.2.1-2016 Robots and robotic devices. Safety requirements for industrial robots. Part 1. Robots

36. GOST R 60.1.2.2-2016 Robots and robotic devices. Safety requirements for industrial robots. Part 2. Robot systems and integration

37. GOST R ISO 26262-1-2014 Road vehicles. Functional safety. Part 1: Vocabulary

38. GOST R ISO 26262-2-2014 Road vehicles. Functional safety. Part 2: Management of functional safety

39. GOST R ISO 26262-3-2014 Road vehicles. Functional safety. Part 3. Concept phase

40. GOST R ISO 26262-4-2014 Road vehicles. Functional safety. Part 4. Product development at the system level

41. GOST R ISO 26262-5-2014 Road vehicles. Functional safety. Part 5. Product development at the hardware level

42. GOST R ISO 26262-6-2014 Road vehicles. Functional safety. Part 6: Product development at the software level

43. GOST R ISO 26262-7-2014 Road vehicles. Functional safety. Part 7: Production and operation

44. GOST R ISO 26262-8-2014 Road vehicles. Functional safety. Part 8: Supporting processes

45. GOST R ISO 26262-9-2014 Road vehicles. Functional safety. Part 9: Automotive Safety Integrity Level-oriented and safety-oriented analyses

46. GOST R ISO 26262-10-2014 Road vehicles. Functional safety. Part 10. Guideline on ISO 26262

47. GOST R 57300-2016/ISO/TS 15998-2:2012 Earth-moving machinery. Machine control systems (MCS) using electronic components. Part 2: Use and application of ISO 15998

48. GOST R IEC 61784-1-2016 Industrial communication networks. Profiles. Part 1. Fieldbus profiles

49. GOST R IEC 61784-3-2015 Industrial communications networks. Profiles. Part 3. Functional safety fieldbuses. General rules and profile definitions

50. GOST R IEC 61784-3-1-2016 Industrial communication networks. Profiles. Part 3-1. Functional safety fieldbuses. Additional specifications for CPF 1

51. GOST R IEC 61784-3-3-2016 Industrial communication networks. Profiles. Part 3-3. Functional safety fieldbuses. Additional specifications for CPF 3

52. GOST R IEC 61784-3-8-2016 Industrial communication networks. Profiles. Part 3-8. Functional safety fieldbuses. Additional specifications for CPF 8

53 GOST R IEC 61784-3-12-2016 Industrial communication networks. Profiles. Part 3-12. Functional safety fieldbuses. Additional specifications for CPF 12

54. GOST IEC 61326-3-1-2015 Electrical equipment for measurement, control and laboratory use. EMC requirements. Part 3-1. Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety). General industrial applications

55. GOST IEC 61326-3-2-2015 Electrical equipment for measurement, control and laboratory use. EMC requirements. Part 3-2. Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety). Industrial applications with specified electromagnetic environment

56. GOST R IEC 61131-6-2015 Programmable controllers. Part 6. Functional safety

About the authors

Alexander F. Kolchin, Deputy Director General, OOO Korporativnie elektronnie sistemy, Russia, Moscow, e-mail: kolchin@calscenter.ru

Oleg S. Yakimov, Director of Regulatory Support, KVF Interstandart, Chairman, Technical Committee for Standardization 058 Functional Safety, Russia, Moscow

Received on 30.06.2017