UDC 656.052:004.056

M. L. MALINOVSKY, D. G. KARAMAN

LLC SPE "Stalenergo", Ukraine

ARCHITECTURE AND IMPLEMENTATION PRINCIPLES OF DATA EXCHANGE EQUIPMENT FOR SAFETY RELATED SYSTEMS

The problem of linking separate subsystems in complex information management systems created and supported by various independent companies is touched upon. The analysis of the key features and differences in safety assurance practices in a variety of management systems is carried out, as well as the possibility of their application in the design and development of linking devices is considered. Principles of construction data exchange equipment between systems having different communication protocols, architecture and safety assurance ideology, while ensuring compliance with the requirements for reliability and safety at the level of alignment are given.

Key words: *control systems; microprocessor centralization; linking devices; data exchange equipment; safety.*

Introduction

Often during development of modern information and control systems several development companies are involved. Each company implements a separate subsystem that interacts with other subsystems through one or more interfaces in accordance with some algorithm and the communication protocol.

System safety requirements are strictly regulated by industry branch, national and international standards [1]. At the same time, each developer has its own special set of methods and tools for the implementation of these requirements. Due to the wide variety of methods and tools used by different companies to ensure safety, it is necessary to solve complex problems when integrating (linking) subsystems from different manufacturers.

As practice shows, the costs of developing data exchange equipment are often comparable to the cost of development of subsystems to be linked. To minimize the costs of the company-partners often are looking for temporary solutions and left relay systems for linking purposes, which results in failing to achieve one of the most important goals of modernization – the exclusion of electromechanical relays that require periodic maintenance.

There are two approaches to solve the mentioned problem. The first is to develop and implement common standards for the construction of interfaces for systems related to security. This approach requires investment of enormous material resources and time spent on processing system architecture and communication protocols from all market participants.

The second way is to develop universal data exchange equipment, which allows adjusting interaction of two or more systems by applying firmware configuration. The creation of such universal linking equipment is the aim of this article.

1. Key features and differences of safety assurance methods, which are used in different control systems

Ensuring the safety of the information and control system operation can be realized on several levels: the level of hardware and data processing units, the information exchange level and the functional-logical level.

At the level of the hardware and data processing units various methods with different options of functional and test diagnosis, redundant duplication methods, the incorporation of the majority circuits are used.

In industrial automation control for designating of the redundancy the special system of notation has been developed. Redundant systems are described by general rule NooM, where N is minimum number of operative items for which the system will be able to perform its task and M – the total number of redundant elements. Letter «D» placed at the end of the formula means that the system has built-in diagnostic tools to concurrently detect and isolate failures that could lead to dangerous malfunctions.

The simplest method to increase the safety of operation is duplication of critical subsystems due to the redundancy scheme described by formula 1oo2. When using duplication the master item of critical subsystem is working in parallel with redundant, that may be either a copy of the first item, or divergent functional analogue. Another widespread scheme – redundant system with double multiplicity, described by formula 2oo3. According this scheme two additional elements are working together with one master element. This method makes it possible to organize a simple voting system based on the majority principle.

In systems with high safety requirements various

types of diagnostic facilities are widely used. The most essential is the functional diagnosis which is carried out during all the time system operates and is able to detect and properly handle failures on-the-fly. Recently, however, due to the increased performance of computing resources of information and control systems, the opportunity to perform a test diagnostics for critical parts during intervals of iteration cycle until they are idle has become feasible. In some cases, for example, when testing the serviceability of the memory elements, non-destructive testing methods are applied.

At the information exchange level data integrity control is performed by calculating checksums or by using error-correcting codes, also as multiple sending repeats, sending data through alternative channels of communication.

Practically all data exchange protocols for industrial communication channels are provided by integrity verification mechanisms based on checksum computation for each transmitted packet or frame. Typically, a checksum length is 8 or 16 bits (1 or 2 bytes) according to data presentation format. The most common types of checksums in general and special purposes telecommunication networks are CRC-8-CCITT, CRC-16-CCITT and CRC-32. There are industry standards to provide integrity, for example, the CRC-7-MVB, used in multifunction vehicle bus (MVB) and train control systems network (TCN) [2, 3]. It is also included in the standard IEC 60870-5 [4], which describes a simple message transfer protocol for remote supervising in distributed information and control systems.

Error detection and correction codes are rarely used because their use leads to a significant overhead of resources and productivity reduction.

At the functional-logical (algorithmic) level the safety is ensured by monitoring the sequence of operations, time control of operations execution, the use of deterministic automata models with irreversible protective states.

Function process of the control system of arbitrary complexity can be described with a finite state automata model. This model implies a certain finite set of states in which the system may remain. The transition between the states is defined by clear rules and it is always possible to determine what is the next state system will switch to from the current state. In addition, the common architecture of real-time systems implies unambiguous, often cyclical sequence of states changing [5]. Thus, providing the system state change control on the algorithmic level could help to prevent the dangerous consequences, if the order of the state change has been broken.

In addition to the cyclical nature of real-time control systems, a strict limitation of the cycle duration should be provided [5]. Each operation is allocated in an appropriate time slot during which all the required actions should be performed. If the time limit is exceeded, it may cause a linking mismatch between control and actuator systems, which, in turn, can lead to dangerous consequences. Independent watchdog timers usually perform time control operations. Timer overflow is a signal to force system suspension and to switch it in safe mode.

2. The principles underlying the architecture of data exchange equipment

Data Exchange Equipment (DEE) is a digital system for collecting, processing and transmitting information through the digital interface and is designed to connect the systems controlling critical technological processes and have different ideology and methods of safety assurance.

One particular application is the use of the DEE as part of theDigital Module of Track Circuits Control (DM TCC) in railway automation systems to provide safe data exchange between the control system (CS) and object controllers (OC).

Before designing the DEE safety concept has been developed, which can be characterized by the following provisions: a single hardware failure should not result in hazardous conditions; single hardware failures, the accumulation of which can lead to dangerous consequences, should be detected and blocked; a combination of single hardware failures should not lead to the emergence of a dangerous condition at a rate exceeding the rate of dangerous failure rate.

Developers provided following measures to ensure the required safety integrity level: hardware redundancy; performing channel self-diagnosis testing by signature verification of crucial software modules in neighbour Logic Core Units (LCU) regardless of the presence or absence of communication between the CS and OC; performing functional verification of neighbour LCU by continuously comparing the generated output data; the use of components with known reliability parameters.

Table 1 summarizes the key characteristics of the systems, linked with the help of the DEE when it is used as part of the DM RCC. The table shows that the ideology of the linked systems has fundamental differences.

DEE consists of four specialized computing modules called Logic Core Units (LCU), which form a dual-channel duplicated structure according to redundancy rule of 1oo2D and two High-level Communication Hubs (HCH) providing a link between LCU and OC (Fig. 1).

Table 1

Key characteristics of the systems, linked by means of DEE

Characteristic	DM RCC	Control system
Redundancy architecture	1oo2D	2oo3
Interface	RS-422	Ethernet
Cycle period	0,1 second	1 second
Safe state criteria	Checksum mismatch (test diagnostic) or output data mismatch (functional diagnosis) at least in one sycle	Mismatch in data processing results in 3 or more cycles out of 10
Criteria of blocking data exchange process from the adjacent system side	None	Data integrity violation in 3 out of 10 cycles

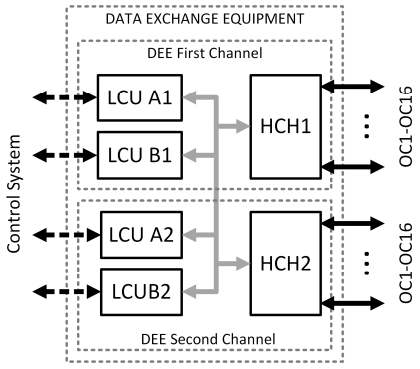

Fig. 1. DEE physical structure

Communication safety between CS and DEE is based on the transmission of information by the majority scheme according to rule 2oo3 with additional protection using CRC-32 checksums. The structure of relationship between the CS and DEE is shown in Fig. 2.

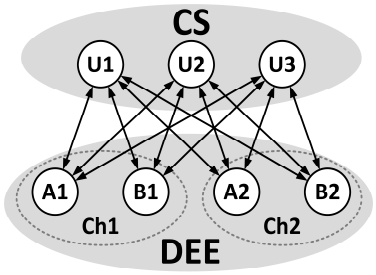

Fig. 2. Interconnection structure between CS and DEE

Each subsystem of the CS generates four packets of control data for each of the LCU that are protected at the application level by 32-bit checksum. Due to the synchronization of received data between LCUs of the same channel and between DEE channels by internal communication lines it is sufficient to obtain consistent packages from at least two CS subsystems by two computing modules of the same channel (totally four packets), in order to handle data as correct and to accept them for further processing.

In response on packets with control actions from CS subsystems each LCU sends control information packet. Each packet is protected at the application level by 32-bit checksum. In order to controlled object data were considered reliable, it is necessary that at least two CS subsystems received valid packets from at least two dissimilar modules (A and B).

If connection with the CS is lost, DEE still remains in operational state and transmits orders of the safe mode on OC.

Each DEE channel can be in the "serviceable", "safe" or "protective" state. Transition DEE channels to a protective state occurs, if there are intermittent failures or transient faults that can be eliminated by resetting the application data or firmware. DEE channel switches to safe state upon detection of permanent failures and persistent faults during a functional or a test self-diagnosis.

DEE can operate in a single channel mode, when only one of the complementary pairs of LCU (A1-B1 or A2-B2) is in serviceable state, and in a dual channel mode according to the redundancy scheme 1oo2D, when both pairs of LCUs are in the serviceable state. Transition of one of the channels to safe state provides automatic switching adjacent channel to a single-channel mode of operation upon lack of inter-channel communication.

Built-in self-diagnosis infrastructure provides testing of critical components at the hardware level. Test self-diagnosis is performed during the operation of the LCU, for which special time slot in the main function sequence is dedicated. Checking critical modules is based on applying an exhaustive set of test actions. During testing output reactions of the module under test are compressed into special signature using CRC-16, which are then compared with similar ones from the neighbour LCU. In case of signatures mismatch DEE channel with detected failure in one of its LCU switches to safe state.

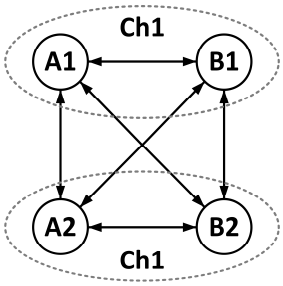

Fig. 3. Structure of interconnections between LCU in DEE

The structure of the internal relationships between LCU in DEE is shown in Fig. 3.

This method of information exchange, called "one with all", can significantly improve the DEE tolerance to failures and defects in communication channels between the CS and DEE, DEE and OC by overloading and alignment of application and service data, as well as the safety of the LCUs through the exchange of self-diagnosis signatures.

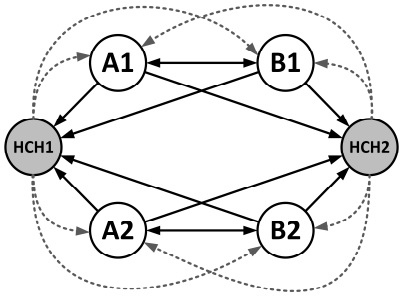

Fig. 4. Structure of interconnections within the DEE

The structure of the interconnections within the DEE, which provides reliable communication between DEE and OC is shown in Fig. 4.

Data exchange between DEE and OC is organized by means of two specialized communication hubs HCH1 and HCH2, which duplicate each other.

3. Practical approval

To prove the stated level of safety conformance an integrated approach was used, including a large variety of methods: expert assessments, reliability and probabilistic calculations, tests on models, testbenches, field tests and statistics in service.

The rate of the hardware failures in modules with self-diagnosis was calculated using Markov chains, based on an exponential distribution law and the failure flow description during time period with a constant failure rate. Calculated values of the key indicators of the EEC reliability ratings are listed in Table 2.

Table 2

Required and calculated values of EEC reliability ratings

Indicator name	Required value	Calculated value
Hardware Failure Rate	1×10^{-12} 1/hour	1.38×10^{-17} 1/hour
Nondetectable Faure Rate in CS-to-OC tract	1×10^{-15} 1/hour	1.11×10^{-16} 1/hour
Nondetectable Faure Rate in CS-to-OC tract	1×10^{-15} 1/hour	8.33×10^{-17} 1/hour

Developed data exchange equipment has been applied for linking the Digital Module for Track Circuits Control (DM TCC) with following centralized systems:

1) control systems, developed by company "Bombardier" – on more than 50 sites in 5 countries;

2) control systems, developed by company "Radioavionika» – on the Vyritsa station of Russian Railways;

3) relay interlocking systems installed in Kharkov, St. Petersburg and the Moscow city underground railways.

Conclusion

In this article a technical solution to the problem of linking sub-systems as part of information and control systems, created and supported by various developing companies using different ideology and safety methods, is presented. The analysis of the key features and differences in safety assurance methods in a variety of information and control systems related to security is carried out. An example of the data exchange equipment for linking such systems is described. Presented Data Exchange Equipment has been widely used for linking the Digital Module for Track Circuits Control with railway automation and control systems of different developers.

References (GOST 7.1:2006)

1. IEC 61508:2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES) [Electronic resource]. – Intr. on April, 2010. – IEC, Geneva. – Access mode: http://www.iec.ch/functionalsafety. – 07.03.2016.

2. Kirrmann, H. The IEC/IEEE Train Communication Network [Electronic resource] / H. Kirrmann, P. A. Zuber // IEEE Micro. – 2001. – no. 2. – P. 81-92. – Access mode: http://www.dca.ufrn.br/~affonso/DCA_STR/trabalhos/rt-diversos/The IEC-IEEE train communication network.pdf. – 07.03.2016.

3. IEC 61375:2012. Train Communication Network. [Electronic resource] – Intr. on June, 2012. – IEC,

Geneva. – Access mode: https://webstore.iec.ch. – 07.03.2016.

4. Clarke, G. R. Practical modern SCADA protocols: DNP3, 60870.5 and related systems [Text] / G. R. Clarke, D. Reynders, E. Wright. – Newnes, 2004. – 537 p. ISBN 07506 7995.

5. Laplante, P. A. Real-Time Systems Design and Analysis: Tools for the Practitioner [Text] / P. A. Laplante, S. J. Ovaska. – John Wiley & Sons, 2011. – 560 p. ISBN 978-0-470-76864-8.

References (BSI)

1. *IEC 61508:2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).* International Electrotechnical Committee, Geneva, 2010. Available at: http://www.iec.ch/functionalsafety. (Accessed 07.03.2016)

2. Kirrmann, Hubert. Zuber, Pierre A. The IEC/IEEE Train Communication Network. *IEEE Micro*, March–April 2001. pp. 81–92. Available at: www.dca.ufrn.br/~affonso/DCA_STR/trabalhos/rt-diversos/The IEC-IEEE train communication network.pdf (Accessed 07.03.2016)

3. *IEC 61375:2012. Train Communication Network*. International Electrotechnical Committee, Geneva, 1999. Available at: https://webstore.iec.ch (Accessed 07.03.2016).

4. Clarke, Gordon R. Reynders, Deon. Wright, Edwin. *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*, Newnes Publ., 2004. 537 p. ISBN 07506 7995.

5. Laplante, Phillip A. Ovaska, Seppo J. *Real-Time Systems Design and Analysis: Tools for the Practitioner*. John Wiley & Sons Publ., 2011. 560 p. ISBN 978-0-470-76864-8.

Надійшла до редакції 11.03.2016, розглянута на редколегії 14.04.2016

АРХИТЕКТУРА И ПРИНЦИПЫ РЕАЛИЗАЦИИ АППАРАТУРЫ СОПРЯЖЕНИЯ СИСТЕМ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

М. Л. Малиновский, Д. Г. Караман

В статье затронута проблема увязки отдельных подсистем в составе комплексных информационно-управляющих систем, создаваемых и поддерживаемых различными компаниями-разработчиками. Выполнен анализ ключевых особенностей и отличий методов обеспечения безопасности в различных системах управления, а также рассмотрена возможность их применения при проектировании и разработке средств увязки. Приведены принципы построения аппаратуры сопряжения систем, имеющих различные протоколы обмена данными, архитектуру и идеологию обеспечения безопасности, обеспечивая при этом выполнение требований к надежности и безопасности на уровне увязки.

Ключевые слова: системы управления, микропроцессорная централизация, средства увязки, аппаратура сопряжения, безопасность.

АРХІТЕКТУРА ТА ПРИНЦИПИ РЕАЛІЗАЦІЇ АПАРАТУРИ СПОЛУЧЕННЯ СИСТЕМ, ЩО ПОВ'ЯЗАНІ З БЕЗПЕКОЮ

М. Л. Малиновський, Д. Г. Караман

У статті порушено проблему ув’язки окремих підсистем у складі комплексних інформаційно-керуючих систем, що створюються і підтримуються різними компаніями-розробниками. Виконано аналіз ключових особливостей і відмінностей методів забезпечення безпеки в різних системах управління, а також розглянута можливість їх застосування при проектуванні і розробці засобів ув’язки. Наведено принципи побудови апаратури сполучення систем, що мають різні протоколи обміну даними, архітектуру і ідеологію забезпечення безпеки, забезпечуючи при цьому виконання вимог до надійності і безпеки на рівні ув’язки.

Ключові слова: системи управління, мікропроцесорна централізація, засоби ув’язки, апаратура сполучення, безпека.

Малиновский Михаил Леонидович – д-р техн. наук, проф., ООО НПП «Стальэнерго», г. Харьков, Украина, e-mail: malinovsky.m@stalenergo.ru.

Караман Дмитрий Григорьевич – инженер, ООО НПП «Стальэнерго», г. Харьков, Украина,e-mail: karaman.d@stalenergo.com.ua.

Malinovskij Mihail Leonidovich – Dr. Sc. in Engineering, Prof., LLC SPE “Stalenergo”, Kharkiv, Ukraine, e-mail: karaman.d@stalenergo.com.ua.

Karaman Dmitrij Grigor'evich – engeneer, LLC SPE “Stalenergo”, Kharkiv, Ukraine, e-mail: karaman.d@stalenergo.com.ua.