Functional Diversity Design of Safety-Related Systems

Ivan Malynyak

Stalenergo LLP
ivanmiros@gmail.com

Abstract. Traditionally, the application of safety voted-groups architectures is a matter of redundancy, where hardware and software components are replicated and become a source of vulnerabilities with decreased system reliability as a whole, therefore necessity of functional diversity design is become essential. Well known diversity approach for similar erroneous results mitigation is widely used, but combined software and hardware techniques to achieve necessary safety system requirements without enlarged implementation of price isn't yet evolved. Avoidance of redundant complexity with limitation the number of channel's internal states could lead to common cause failures reduction and sufficient level of residual risks.

Keywords. fault tolerant architecture, 1oo2D, 2oo3, redundancy, complexity, control systems, diversity, common cause failures

Key terms. Process, Technology, Development, Reliability, SoftwareComponent

1 Introduction

Nowadays technology of control system is believed to be effective and safe, where essential approaches are sufficiently exploited [1]. The current generation of instrumentation and control systems is highly integrated digital complexes which offer better performance, versatility and additional diagnostic capabilities in comparison with aged analog systems. But as far as systems become more safety-critical, all kinds of possible vulnerabilities have to be taken into account.

This paper offers the concept of functional diversity design which is unfolded by three steps from the problem, through different approaches to the implementation. First of all, necessity of latent systematic faults elimination is assumed, where question of misinterpreted functional requirements within the system becomes a main framework for modern applications [2, 3]. Secondly, the approach to cover up to 99.9% faults without overhead in performance and power consumption based on modern surveys is suggested [4]. And finally, new architecture based on reduced system complexity which helps to make up savings in development life cycle stage with higher availability and higher safety in railway industry is proposed.

To be accurate with terminology, the functional diversity design in this paper is not assumed as different physical functions within determined process implementation, but more broadly, where fundamental diverse technology is considered in a way of inherent difference without any commonality in its nature. Even the most comprehensive strategies approach are suffered from the common channel failures and possible external influences or insufficient faults mitigation that can further contribute to the potential concurrent vulnerabilities [2]. Indeed, all mentioned strategies assumed the six different fault management techniques which solves equal project problems in redundant channels, composed of sensors, computers and control elements with purpose to take the process to a de-energized state when predetermined conditions are violated.

As shown in Fig. 1, two types of well-characterized redundant architectures (2oo3 and 1oo2D) have equal functional structure schemes A$\Leftrightarrow$B$\Leftrightarrow$C and therefore cycle's synchronization procedures within sub-channels are required. As a result, extra data connection lines between sub-channels are used to establish additional information exchange and projects very often become fed up with wiring L and sophisticated inter-channel redundancy management.

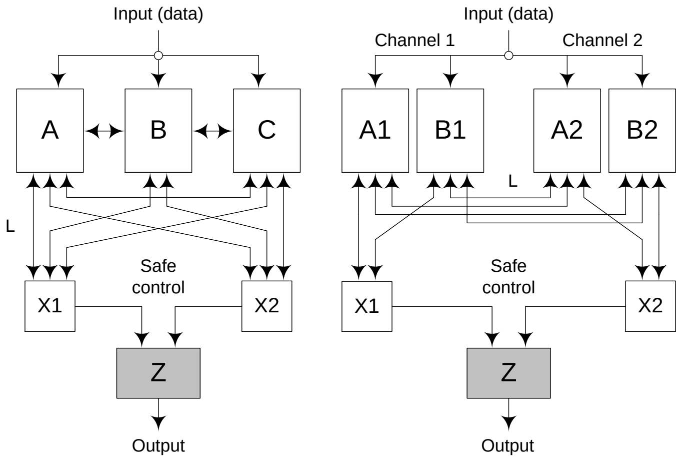

Fig. 1. Two types of well-characterized architectures 2oo3 (left) and 1oo2D (right)

Almost all created inter-channel data than is sent to hardware/software redundant voting mechanism Xi which than implements safe control output function Z. Despite the fact that diversity questions are deeply concerned and surveyed, the biggest issue still lies in assumption of equal channel functional design, where the fundamental problem took their roots [4, 5]. Of course, it's easy to fit out the system with all kinds of diversity techniques, but absence of overall differential approach can't guarantee prolonged operation without common cause vulnerabilities. The possibility of concurrent triggering the latent multi-channel failures is potentially hazardous and it's like a group of man walking simultaneously around a pit with averted eyes.

The way out could be found in “sequential” (or satellite) type of system architecture, where parallel equivalent sub-channels are substituted with diverse ones as shown in Fig. 2. The challenge is to cope with nature evolution, where necessity of redundancy implements as sequential algorithm in embedded bundle of diverse entities [6]. The idea is already has been considered in [2], but existent architectural context is still repeated virtual “OR” logic of distinct sub-channels. Even if functional diversity is achieved through different control laws, elements and distinct functionality, the need of overall agreement among the sub-channels and data synchronization may critically affect output values.

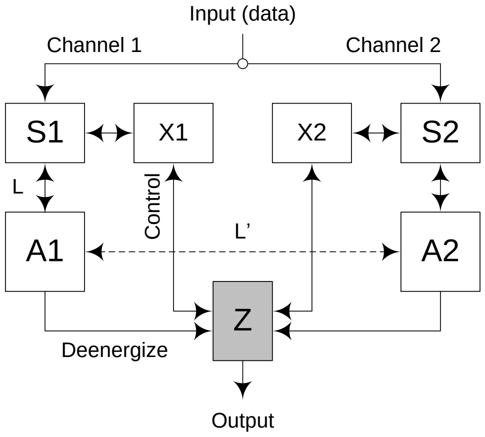

Fig. 2. Sequential architecture of safety redundant control systems 1oo2S

Data lines in sequential architecture 1oo2S are minimized to essential level with safety functions are guaranteed to be executed correctly by de-energize signals. This type of architecture isn’t widespread despite advantages of system simplicity because of general established multichannel parallel approach used to cover safety issues. Nevertheless, such direction may have its future in the light of necessity to drop overall system complexity to acceptable level for commercial use.

2 Redundancy

The challenge of providing redundancy management to meet certain requirements for different application is complicated by the critical constraints of market cost and schedule. Further evolution of redundancy management with its intricate synchronization interfaces and overall complexity were already found to be potentially catastrophic [7]. This approach obviously was costly in a way of wiring and components but from the other hand it’s offered rather simple and attractive macro level “black box” design.

As one could see, the redundancy approach is well known and understandable, where failures of elements could be easily found by comparison. For simple functions it works greatly and reliability decreasing is not matter of consideration. But when dozens of input and output were designed with redundancy management, cost of developing and physical implementation tended to increase exponentially. The result of complexity already known and contained to be in faults propagation which leads to unsafe concurrent failures of two or more identical parallel sub-channels [8].

More than that, the design to achieve necessary safety level leaded out into duplicating functions almost at every step. Firstly, the safe input means at least of two signals to be monitored with safe outputs are based on the same repeating principal. Secondly, to achieve availability requirements the “design shape” just went on adding next “channel 2”, but of course it could be more channels. And finally, when all components are successfully placed, the intricately net of data communicating has to be put over.

The first step down from “black boxes” design could be avoiding some needless redundancies. As shown in Fig. 3, 1oo2D architecture is looked safe due to transparent functional scheme. Indeed, all inputs are duplicated and could be verified by other neighbor. Moreover, output Z is drove from two channels by voting mechanisms Xi, with ability to perform safety de-energized state.

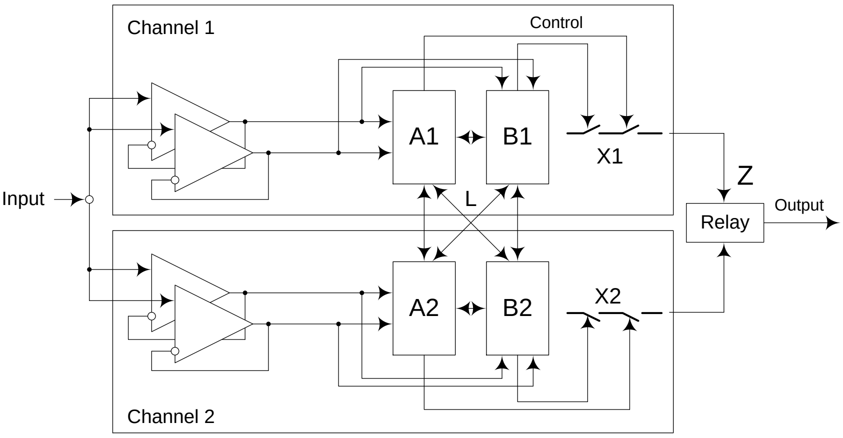

Fig. 3. Decomposition of 1oo2D architecture

On the contrary, the sequential architecture approach could change the whole appearance of system design, where redundancy eliminating is only the first step to be done. As shown in Fig. 4, the point of view lied in the basic sequential approach idea, where elements of system are presented with non-symmetrical faults property. Let’s describe it by simplified hardware model, which could be than enlarged on software issues by substitution physical elements with similar software routines in a project.

For example, if “input” is implied as thermocouple, than implementing fixed current with periodical caliber testing would guarantee possible input faults detection. Indeed, the only fault is not detected by this approach is a rare gradual measurement drift and by using high quality thermocouple with periodical external checkup this could be solved and particular problem due to low possibility of such fault would be eliminated. As a result, a thermocouple with measuring circuits is treated as single element with non-symmetrical types of faults, where most likely defects in circuit break or rapid measurement drift (op-amps or connecting line issues) are easily detected. The non-symmetrical type fault output is treated in the same way, where satellite sub-channel S drives relay Z safely through transformer X with inherently eliminating shortcut failures. The main sub-channel A is connected to S with communication line where control data and both functional integrity is transferred. Each of sub-channels could run safety function by de-energizing transformer in case of discrepancy.

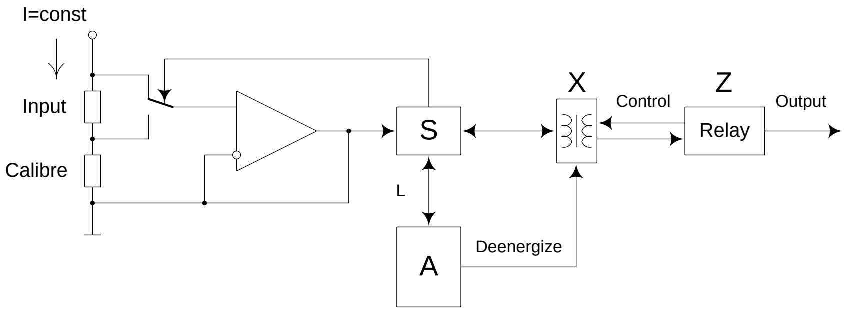

Fig. 4. Simplified model of sequential architecture 1oo1S

As a result, sequential approach is constrained to build the system with strong functional design separation between core algorithm A and routine input/output tasks, whereupon for example the fast and simple satellite sub-channel S is prepared to deal only with input/output X and functional integrity management. The effect would come out of overall system complexity reduction, common cause failures elimination and reliability enlargement due to algorithm simplification with functional diversification.

3 Design of safety-related systems

The main aim of diversity is to perform safety functions achieved by monitoring the behavior of number of sub-channels. The way safety ideas are implemented reminds “fractal” pattern, where general method of reiteration is repeated at every scale of a project. It could be seen in software, where developer has no idea how his source code would be eventually implemented into assembler language. The same thing is happened in hardware, where design is implemented by pure repeating elements based on monolithic integrated circuits without clear understanding of its full functionality. As a result, each level of system decomposition is considered with increasing uncertainty and the principle of aggregation with uncontrollable elements cascading may not be as reliable as it expected.

Finally, the result of uncontrolled “fractal” implementation is come out as necessity of channel diversity due to providing predictable system behavior and is turned to entity multiplication which has to be carefully verified [9]. Hereafter, when system is installed, a well known golden rule is remained - “don’t change anything”.

Evolution of Nature shows that repeated and uncontrolled growth ultimately leads to disaster, just look back on dinosaurs or cancer. So, the main idea of safety may lies in capability of system predicting its behavior with reasonable complexity. For example, for the implication to the brain size it could be said, that decision making mechanism should be “large as you need and as small as you can” [10].

Looking forward at systems design, there is a time point when sufficient data of failures is gathered and overall availability could be increased just due to better maintenance understanding. Indeed, if its clear how light bulbs in mines are breaks and what circumstance is preceded, then particular algorithm with appropriate feedback could lead to limited abundance of lighting control system or even eliminate redundancy at all due to accurate prediction of failures with using certain planned actions.

After thorough revision of prevail railway control systems it’s assumed, that architectures could be transformed into simplified 1oo2S variant, where all inputs and outputs are designed with proper feedback (shown in Fig. 5).

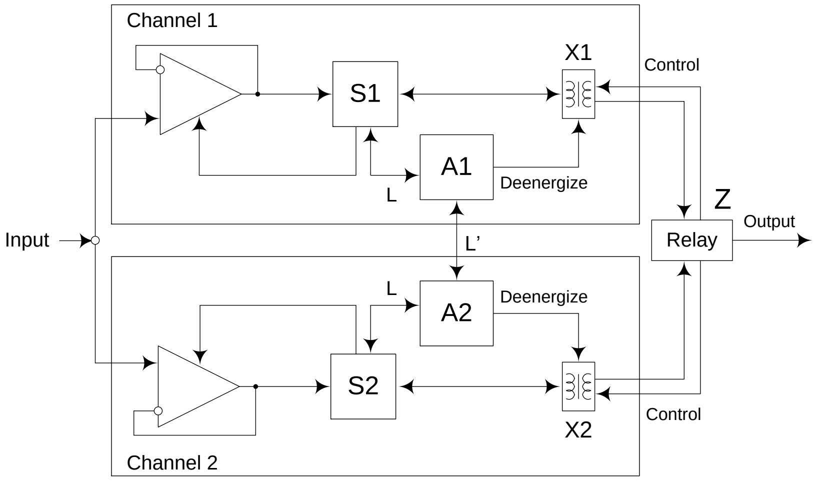

Fig. 5. Decomposition of 1oo2S architecture

For the preliminary evaluation of design safety advantages, it’s assumed that set of proper input signals $p \in P$ or faults $q \in Q$ are used for all sub-channels A,B,C with set of internal conditionals $r \in R$ to implement safely output set Z or hazardous output set Z’.

For 1oo2D architecture $A \Leftrightarrow B$ is assumed where diversity mechanisms within sub-channel could be implemented or not. Working states when safety function operates normally is described by formula:

$$\forall\, r,p\text{: } Arp=Brp,\ Z \wedge Z' = \varnothing \qquad (1)$$

Nonworking de-energized output state where sub-channels' internal conditions are differ because of failure detection:

$$\exists\, r,q,p\text{: } Arq \neq Brp \vee Arp \neq Brq,\ Z = \varnothing \qquad (2)$$

Hazardous state where sub-channels' outputs synchronously being changed by latent failure:

$$\exists\, r,q\text{: } Arq=Brq,\ Z \wedge Z' \neq \varnothing \qquad (3)$$

Sequential architecture 1oo2S is considered to be diverse on design level where each sub-channel is used different technologies, logic and way of responding by nature, therefore equation $A \wedge S \approx \varnothing$ is assumed. Nevertheless, in order to provide necessary safety technique, the idea of artificially divided sub-channels' internal conditionals alphabet is used and proper mapping of normal responses set within each sub-channel is determined [11]:

$$\forall\, r,p\text{: } Arp \subseteq S_A \wedge Srp \subseteq A_{S,}\, Z \wedge Z' \approx \varnothing \qquad (4)$$

Here the SA is a set of sub-channel A mapping responses which are analyzed in S and vice versa. Hazardous state where sub-channels' outputs synchronously being changed by latent failure are very rare due to functional diversity design:

$$\forall\, r,p,q\text{: } Arpq \wedge Srpq \approx \varnothing \qquad (5)$$

In order to avoid potentially hazardous states, a number of conditions must be met [2]. Let us assume A and S with internal symmetric difference feature and in theory it's possible to reach necessary level of identified errors possibility at 99.9%:

$$\forall\, r,p,q\text{: } Arpq \Leftrightarrow \neg\, Srpq_{,}\, Z \wedge Z' \approx \varnothing \qquad (6)$$

One of the approaches to achieve channels' software symmetric difference could be based on "likely program invariants" idea with substitution invariants property of critical parts for negations ones [12]. For example, if sub-channel A algorithm has CASE operator for "what must be done", than sub-channel's S algorithm to control this part of software should have operator for "what is not supposed to be done in any case".

This paper is regarded only as intention where distinguish functional design specifications of sub-channels is took into account. The formulas (1-6) are correlated with already developed theoretical foundation and mathematical models of multi-version systems [11], where different diversity kinds $r \in R$ are sequentially accumulated in final diverse versions by special mapping of output signal set $Zi \rightarrow Z$.

4 Architecture diversity usage

The problem of common cause failures mitigation basically could be found in four industries (aviation, chemical process, rail transportation and nuclear power plant) that provide high failure-consequence consideration in evaluating the diversity.

The usage of diversity are described in [2] with guidance related to clear examples of diversity (shown in Table 1).

Table 1. Summary of diversity usage

Diversity	Aviation	Railway		Chemical	NPP
Equipment	x		1oo2S	x	x
Design				x	x
Function	x	x		x	x
Human	x	x		x	x
Signal		x		x	x
Software	x	x		x	x

In spite of the intensive researches in area of multi-version systems, the distributed nature of the rail network and the localized action for interlocks and train control, the railway safety management is paid less attention to diversity implementation. By stopping or slowing trains to inhibit access to occupied tracks, railways have a readily accessible safe state by local de-energized “stop” configuration. This failsafe approach based on old all-relay interlocking system resulted in a practical emphasis for identifying faulted conditions and stopping the affected trains until the hazard can be cleared.

In the modern microprocessor interlocks and train control the system diversity usage is vital due to increased speed and shortened time between rolling-stocks. Moreover, unique set of input and output signals for every railway station imposed additional constraints on control systems, which has to be flexible in configuration, safe in operation and cost effective in realization.

The idea of sequential 1oo2S architecture could fill the diversity gap in domains, such as traffic control, where collision avoidance is a key of operational safety but with considerable economic constraints.

5 Conclusions

With respect to size and complexity of modern safety-critical application it could be assumed, that one way to achieve necessary system requirements without enlarged implementation price is functional diversity design optimization. This paper proposes combined software and hardware applying, where overall system complexity would not exceed the uncontrollably high level and would decrease developing time.

Sequential safety architecture 1oo2S combines the benefit of 1oo2D and 2oo3 systems with higher availability and higher safety levels. The price for this innovation lies in additional functional requirements to successfully analyzing integrity of sub-channels. The additional benefit from such approach could be significant protection against vulnerability of most common cause failures when software design shortcomings and hardware faults are came to light.

References

1. IEC 61508-3:2010: Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems – Part 3: Software Requirements
2. Wood, R.; Belles, R., Cetiner, M. & et al. Diversity Strategies for NPP I&C Systems, NUREG/CR-7007 ORNL/TM-2009/302, (2009)
3. Yastrebenetsky, M., Kharchenko, V.: Nuclear Power Plant Instrumentation and Control Systems for Safety and Security. IGI Global, (2014).
4. Yoshikawa, H., Zhang, Z.: Progress of Nuclear Safety for Symbiosis and Sustainability: Advanced Digital Instrumentation, Control and Information Systems for Nuclear Power Plants. Springer, Japan, (2014)
5. Avizienis, A., Laprie, J.-C., Randell, B.: Fundamental Concepts of Dependability. Research Report No 1145, LAAS-CNRS, (2001)
6. Mukai, Y., Tohma, Y.: A Method for the Realization of Fail-Safe Asynchronous Sequential Circuits. IEEE Trans. Computer. 23(7), 736–739, (1974)
7. Boykin, J., Thibodeau, J., Schneider, H.: Evolution of Shuttle Avionics Redundancy Management/Fault Tolerance. Space Shuttle Technical Conference, NASA Conference Publication 2342. Part 1, Johnsons Space Center, Texas, pp.1–18, (1983)
8. Madden, W., Rone, K.: Design, Development, Integration: Space Shuttle Primary Flight Software System. Communications of the ACM 27(9), 914–925, (1984)
9. Astrom, K., Murray, R.: Feedback Systems: an Introduction for Scientists and Engineers. Princeton Univ. Press, (2008)
10. Davidson, I.: As Large as You Need and as Small as You Can: Implications of the Brain Size of Homo Floresiensis. In Schalley, A., Khlentzos D.: Mental States. V.1: Evolution, function, nature, pp. 35–42, (2007)
11. Kharchenko, V., Siora, A., Sklyar, V.: Multi-Diversity Versus Common Cause Failures: FPGA-Based Multi Version NPP I&C systems, Proceeding of the 76th conference NPIC&HMIT, Las-Vegas, Nevada, USA, (2010)
12. Sahoo, S., Li, M., Ramachandran, P., Adve, S., Adve,V., Zhou, Y.: Using Likely Program Invariants to Detect Hardware Errors. In Conf. Dependable Systems and Networks – DSN, pp. 70–79, (2008)