Copyright © 2002 IFAC
15th Triennial World Congress, Barcelona, Spain

WHAT IS RELIABLE CONTROL?

Koichi Suyama [*]

[*] *T okyo University of Mercantile Marine*
Koto-ku, Tokyo 135-8533, Japan
E-mail: suyama@ipc.tosho-u .ac.j p

Abstract: Reliable control has been brought to attention by its contribution to system design according to the international standard on system safety, IEC 61508. This paper systematizes reliable control by clarifying its essence and meaning in accordance with the policy of IEC 61508. The systematization is indispensable for its further advances as the social environment surrounding system safety hopes.

Keywords: Safety, risk, fault-tolerant systems, standards.

1. INTRODUCTION

Since Šiljak firstly used the term *reliable control* in the late 1970s, many studies have simultaneously and independently been made on control system design under possible device failures, such as integrity (Fujita and Shimenura, 1988; Gündes, 1992; Sebe, 1996; Hamada *el al.*, 1996), reliable H_∞ control (Veillette *el al.*, 1992; Veillette, 1995; Yang *et al.*, 1998) and passive redundancy (Vidyasagar and Viswanadham, 1985; Minto and Ravi, 1991). At the 33rd IEEE CDC and at the 2001 ACC, the technical session "Reliable control" consisting of papers in the above research areas was set up. However reliable control has not been systematized well. Its essence and meaning have not been discussed and clarified until now. Even Šiljak (1995) regarded reliable control as only one area in stability theory.

On the other hand, over the past decade the social environment surrounding system safety has changed rapidly, as you can see in Health & Safety Executive (1995). One of the epochs was that TC65 WG9&10 in IEC, International Electrotechnical Commission, established an international standard, IEC 61508 (1998–2000). It is applied to almost all electrical/electronic/programmable electronic safety-related systems irrespective of their applications. It has been already quoted into several national standards or guidelines of UK, USA and Japan, including those for process, aerospace and railway transportation sectors.

The important point to note is that reliable control has been brought to attention by its contribution to system design according to IEC 61508. This paper systematizes reliable control in accordance with the policy of IEC 61508. Although reliable control is now making advances, the systematization is indispensable for its further and great advances as the social environment surrounding system safety hopes.

2. ESSENCE OF RELIABLE CONTROL

2.1 Example

Consider a disturbance attenuation problem for a plant consisting of two actuators susceptible to failures, a controlled object and three sensors. Suppose that a generalized plant is given by

$$\frac{d}{dt}x(t) = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{bmatrix} x(t) + \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} u(t) + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} w(t)$$

$$y(t) = x(t)$$

$$z(t) = \begin{bmatrix} 2 & 2 & 0 \\ 1 & 0 & 1 \end{bmatrix} x(t) + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} w(t).$$

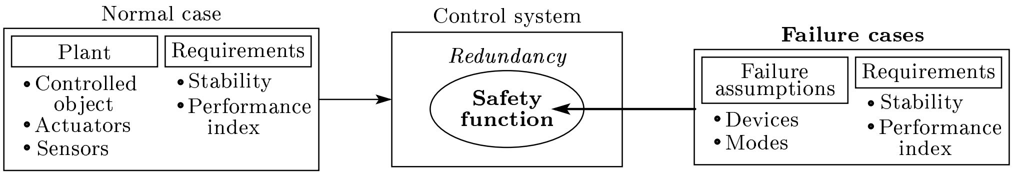

Fig. 1. Reliable control.

The disturbance attenuation performance is evaluated by $\|T_{zw}\|_2$ where T_{zw} is the transfer function from the noise $w(t)$ to the performance output $z(t)$, and $\|\cdot\|_2$ denotes H_2-norm. Consider the following two design results of state feedback

$$u(t) = Fx(t).$$

Design 1: Solving a full-information two-block H_2 problem to minimize the performance index, we have

$$F = \begin{bmatrix} -2.17 & -2.67 & -0.79 \\ -1.79 & -3.12 & -4.66 \end{bmatrix}.$$

Table 1(a) shows the property of the obtained control system. The sufficiently small performance index in the normal case implies that the obtained control system has desirable disturbance attenuation performance. However, if either actuator fails and loses its function, the control system falls into an unstable situation.

Table 1. Design results.

(a) Design 1 (H_2 optimal design).

Case	Normal	Actuator 1 failure	Actuator 2 failure
Poles	-1.91	0.43	1.94
	$-1.46 + j0.69$	-0.72	-1.99
	$-1.46 - j0.69$	-2.37	-0.13
$\|T_{zw}\|_2$	6.50	—	—

(b) Design 2 (reliable control).

Case	Normal	Actuator 1 failure	Actuator 2 failure
Poles	-10.56	-3.11	-2.88
	$-0.39 + j0.12$	$-0.63 + j0.18$	-1.62
	$-0.39 - j0.12$	$-0.63 - j0.18$	-0.47
$\|T_{zw}\|_2$	32.00	61.49	66.14

Design 2: Consider

$$F = \begin{bmatrix} -6.97 & -10.17 & -13.56 \\ -3.70 & -5.00 & -6.37 \end{bmatrix}.$$

Although the disturbance attenuation performance in the normal case is worse as compared with Design 1, the stability of the control system can be maintained even if either actuator fails as shown in Table 1(b).

In the ordinary control system design, we look for and obtain the best normal-case performance, e.g., stability and control performance evaluated by a performance index, while on the other hand the obtained control system may be weak against device failures as in Design 1. Reliable control realizes safety function against device failures in the control system at the sacrifice of the normal-case performance as in Design 2.

2.2 Safety function in redundancy

The essence of reliable control can be summarized as shown in Fig. 1.

- Under the assumption that possible device failures drive a control system to an undesirable situation, failure-case performance, besides the normal-case performance, is taken into consideration.
- Safety function against the assumed device failures is realized in redundancy existing in the normal-case control system.

In the example in Section 2.1, the two failure-assumed actuators operate simultaneously and independently in the normal case. Note that one is not a backup for the other. If one fails and loses its function, the normal other makes up the failure to maintain the stability of the control system. That is, safety function is realized in the form of mutual aid function between the two actuators.

The important point here is that there exists redundancy in a control system in a broad sense. In the example in Section 2.1, the two actuators are used, where each can stabilize the control system by itself. It is not necessary to use both simultaneously unless we look for extremely high control performance. That is, there exists redundancy. Then, as in Design 2, we can realize safety function in the form of mutual aid in the redundancy.

In general, redundancy in the sense of productivity or efficiency is indispensable to realize safety function in a control system. Note that safety devices based on fault detection/diagnosis are also redundant in such sense, as mentioned in Section 3.2.

Even if there exists redundancy in a control system, it is not easy to realize safety function effectively in the redundancy. In the example in Section 2.1, the safety function in the form of the mutual aid is that each actuator can control the controlled object by itself. On the other hand, another type of mutual aid function, cooperation, is needed in the normal case. That is, in the normal case where both actuators operate, the control system may fall into an unstable situation unless they cooperate effectively. To make good use of redundancy existing in a control system, we should design so that such various requirements shown in Fig. 1 are simultaneously satisfied. Reliable control is just the theory to give such a design.

2.3 Distinctive feature

Safety function realized by reliable control exists and operates in a control system in the normal case. Once failure-assumed devices fail, the built-in and hidden safety function gives full play to its ability to maintain the performance with its admissible deterioration. That is, emergency measures are automatically taken by the safety function without any urgent detection of the failures. It is sufficient that the failures can be detected while the safety function operates effectively.

In the ordinary fault-tolerance framework, emergency measures are taken after detection of failures. That is,

- a failure should be detected as soon as possible after its occurrence, and
- emergency measures based on the detected information maintains the performance including the stability.

Fault detection plays the most important and essential role. It is imposed a severe burden.

On the other hand, reliable control can lighten the burden imposed on fault detection. It is one of the remarkable features of the safety function realized by reliable control that emergency measures are automatically taken by the built-in and hidden safety function, without detection of the failures.

2.4 Relation with robust control

Reliable control has a resemblance to robust control. Treating assumed device failures as plant perturbation, we can design a control system so that it is stable against the perturbation. It has been often said that reliable control belongs to the category of robust control. However it is not strictly true. Such a fallacy is an obstruction to advances in reliable control.

It is certain that the problem formulation and design methodologies in robust control can also be used in reliable control. However it is only a makeshift and temporary step taken in the theoretical advances in reliable control. The ultimate goal of reliable control is to present safety function against *discrete* failure situations caused by device failures, such as device failure contexts (Suyama and Apostolakis, 2000; Suyama and Apostolakis, 2001; Suyama, 2001). Such situations should be discriminated from *continuous* perturbation considered in robust control. Reliable control is close in meaning to simultaneous stabilization/control rather than robust control.

2.5 Place in fault-tolerance technology

Of course, reliable control is one field of fault-tolerance technology. Fault-tolerance technology includes extremely wide range of fields, such as error detecting codes. Hence it is important to clarify the place of reliable control in fault-tolerance technology.

As mentioned before, reliable control is a design theory for realizing safety function in redundancy existing in a control system without urgent detection of failures. This is a contribution to fault-tolerance technology from control system design. It is important to note the difference between the safety function realized by reliable control and fault-tolerance based on fault detection as in the ordinary fault-tolerance framework. As mentioned in Section 3, they should be discriminated in accordance with the policy of IEC 61508.

3. MEANING OF RELIABLE CONTROL

3.1 Functional safety

In IEC 61508, safety measures are evaluated from a standpoint of risk reduction in accordance with ISO/IEC Guide 51 (1990).

Figs. 2 and 3 illustrate the overall system configuration and its risk reduction considered in IEC 61508. The original control system consists of

- equipment under control (EUC): equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities, and
- basic control system (BCS): system which responds to input signals from the process and/or an operator and generates output signals causing the EUC to operate in the desired manner.

IEC 61508 requests to reduce the initial risk of the original control system by the following measures so that the residual risk of the overall system is less than the predetermined tolerable risk level.

- Safety-related systems (SRSs): systems that implement the required safety functions necessary to achieve or to maintain a safe state for the EUC.

    - Electrical/electronic/programmable electronic (E/E/PE) SRSs: SRSs based on E/E/PE technology.
    - Other technology SRSs: SRSs based on other technologies.
- External risk reduction facilities (ERRFs): physical measures taken external to SRSs to reduce or mitigate the risk.

To be precise, IEC 61508 is the international standard for E/E/PE SRSs.

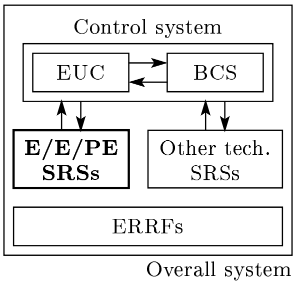

Fig. 2. Overall system considered in IEC 61508.

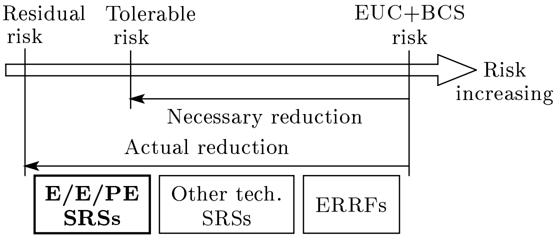

Fig. 3. Risk reduction.

Table 2. Safety integrity levels.

(a) Low demand mode of operation.

SIL	Average probability of failure to perform its design function on demand
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

(b) High demand/continuous mode of operation.

SIL	Probability of a dangerous failure per hour
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

An SRS, just like a safety device, has safety function to achieve or to maintain a safe state of the EUC. Functional safety is its ability to perform the safety function.

Note that a hardware failure occurs at a random time in an SRS. Then there is the possibility that the SRS cannot perform its safety function. IEC 61508 evaluates functional safety of an E/E/PE SRS, i.e., the probability of failure to perform its safety function, using four safety integrity levels (SILs) for two kinds of operation modes. If an SRS shoulders a heavy burden for risk reduction, it is required to fit a higher SIL.

IEC 61508 applies SILs in high demand/continuous operation mode shown in Table 2(b) to an SRS inside a control system, i.e., inside a BCS. If the probability of a dangerous failure, where safety function realized by reliable control in a BCS is lost, is less than 10^{-5}[1/hour], the BCS itself is regarded as an SRS. Then IEC 61508 should be applied to the BCS.

3.2 Safety-related systems outside a control system and reliable control

Compare an SRS outside a control system (O-SRS) and reliable control in their functional safety. Because an SRS can exists inside a control system, as mentioned above, it is necessary to discriminate between such an SRS and an O-SRS.

Table 3 summarizes the comparison.

Firstly, both are based on E/E/PE technology. As mentioned before, IEC 61508 is an international standard for E/E/PE SRSs. Reliable control is a design theory for control using digital controllers and control devices such as sensors and actuators, which are also based on E/E/PE technology.

As mentioned in Section 2.2, in general, safety function is realized in redundancy of a control system in the sense of productivity or efficiency. In the overall system considered in IEC 61508 shown in Fig. 2, O-SRSs installed newly for risk reduction themselves are redundant. They demand extra costs.

On the other hand, reliable control uses the existing redundancy in a control system. In most cases reliable control realizes safety function against device failures in the redundancy at the sacrifice of the normal-case performance, as in the example in Section 2.1. One of the merits of reliable control is to keep extra costs down.

Next, compare them in their safety function. Although an O-SRS always monitors the condition of a control system, it is a stand-by system operating only in case of need. If it receives the information from the sensors for its exclusive use that there is the indication that a control system falls into a dangerous situation, it immediately operates the actuators for its exclusive use for emergency measures.

However, if there is a hidden failure in the sensors, the dangerous indication is detected late or cannot be detected. If there is a hidden failure in the actuators, sufficient emergency measures are not taken against the dangerous indication.

Table 3. Safety-related systems outside a control system and reliable control.

	O-SRSs	Reliable control
Redundancy	Outside a control system	Existing in a control system
Sacrifice for safety function	Costs	Normal-case performance
Safety function in normal case	Stand by	In operation
Safety function	Detection → Measures	Measures → Detection
Reason for failure of safety function	Hidden failures	Late detection
Mode of operation	Low demand mode	Continuous mode
Proof tests	Necessary	Unnecessary

It is necessary that an O-SRS has sufficient self-diagnosis function and that proof tests are carried out so that there is no hidden failure in the O-SRS.

To evaluate functional safety of such an O-SRS, IEC 61508 applies mainly the SILs in low demand mode of operation. There are some O-SRSs which, for special reasons, the SILs in high demand mode of operation should be applied to.

Safety function realized by reliable control exists and operates in a control system in the normal case. Once failure-assumed devices fail, the built-in and hidden safety function gives full play to its ability and maintains the performance with an admissible deterioration. That is, emergency measures are automatically taken by the safety function without any urgent detection of the failures. It is sufficient that the failures can be detected while the safety function operates effectively.

Conversely, if the failures cannot be detected before another non-assumed failure occurs, the safety function realized by reliable control fails to perform. Hence it is necessary to evaluate the functional safety realized by reliable control from such a viewpoint as in Suyama (1999). Here, because the safety function operates in the normal case., IEC 61508 applies the SILs in continuous mode of operation to the functional safety.

If an assumed failure occurs, it should be detected and repaired. However it is not necessary to confirm that there is no hidden failure by operating some devices specially. The safety function realized by reliable control does not need proof tests.

3.3 Reliable control for risk reduction

As compared in Section 3.2, an O-SRS and reliable control definitely differ in their properties, merits and demerits. Because it is sufficient that risk reduction shown in Fig. 3 is performed as the overall system shown in Fig. 2, they can be complementary to each other as shown in Fig. 4.

Revisit the example in Section 2.1. Due to the functional safety realized by reliable control, the risk of the control system EUC + BCS 2 obtained by Design 2 is less than the risk of EUC + BCS 1 obtained by Design 1. Hence, when we reduce the risk of the overall system so that the residual risk is less than the tolerable risk, a lighter burden is imposed on O-SRSs in the case of EUC + BCS 2. For example, you can imagine that an O-SRS of SIL 2 is sufficient for the control system EUC + BCS 2 while the control system EUC + BCS 1 needs an O-SRS of SIL 3 or 4. Reliable control can be complementary to an O-SRSs.

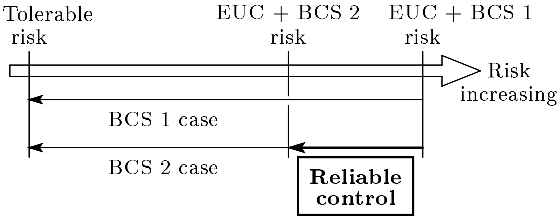

Fig. 4. Necessary risk reduction.

There are several limitations on realizing safety function by reliable control, such as redundancy existing in a control system and its effectiveness. However we should try to use positively reliable control if it can contribute to risk reduction.

The importance of safety function realized in a control system has been growing for the last several years. One of the reasons is that ISO/IEC Guide 51 (E; 1999) adopted newly risk for environment and risk for properties as its scope. It is widely known that there are many cases where SRSs and ERRFs are not enough to reduce the risk for environment/properties. The Japanese Core Users Interest Group (J-CUIG; Core Users Interest Group, 2000)[1] regards highly reliable control as one of the key techniques for realizing safety function in a control system.

Remark 1: It is important that a BCS and an O-SRS do not have common components to avoid common-cause failures. However actually there are many cases where they have common components such as sensors and actuators. In such cases we should pay more attention to the realization and the evaluation of the complementarity in risk reduction between an O-SRS and reliable control.

4. FUTURE DIRECTION

A great deal of effort in reliable control will be made on the consistency with other research areas

[1] The author is a member of J-CUIG.

on system safety because the gap between them cannot be ignored. For example, the term *integrity* indicates an idea of fault-tolerant stability in reliable control. However, as you know, it has another meaning in the field of reliability engineering. The system structure *passive redundancy* in reliable control is called *active redundancy* in the field of reliability engineering (Smith, 1997). We should pay our attention to the consistency with other research areas.

Context-based approach (Suyama and Apostolakis, 2000; Suyama and Apostolakis, 2001; Suyama, 2001) is one of such studies.

Probabilistic Risk Assessment (PRA; Henley and Kumamoto, 1992) plays an important role in safety analysis of safety-critical control systems, such as nuclear power plants and chemical processes. An idea of contexts is essential in PRA, which specifies the total situation of a system, i.e., normal/failure situation of each device and physical state of the system (Garrett and Apostolakis, 1999). PRA analyzes the safety of a system to present information on critical contexts which need safety measures. Based on the information, we design, redesign, or improve the system.

In such reliable control as integrity and reliable H_∞ control, the device failure cases to be considered are all combinations of failures in some specified devices. Hence the conventional reliable control is not consistent with PRA.

Context-based approach is a new framework of reliable control to make the best use of the analysis results given by PRA. Only the device failure cases included in critical contexts given by PRA, device failure contexts, are treated directly. We design a controller for the measures against them, taking the following into consideration.

- Performance in contexts: Context-dependent performance index (Suyama and Apostolakis, 2001) changes with the device failure cases so that it can reflect the system performance appropriately.
- Priorities of contexts: Contexts including the normal case should be treated in accordance with their priorities (Suyama and Apostolakis, 2001; Suyama, 2001).

The controller design is reduced to the standard H_∞ problem. It is for practical use in the design-analysis iteration with PRA.

REFERENCES

Core Users Interest Group (2000). The Japanese Core Users Interest Group (J-CUIG). *Epigram*, Autumn 2000.

Fujita, M. and E. Shimemura (1988). Integrity Against Arbitrary Feedback-loop Failure in Linear Multivariable Control. *Automatica*, **24**, 765–772.

Garrett, C. and G. Apostolakis (1999). Context in the risk assessment of digital systems. *Risk Analysis*, **19**, 23–32.

Gündeş, A.N. (1992). Stability of feedback systems with sensor or actuator failures: analysis. *Int. J. Control*, **56**, 735–753.

Hamada, Y., S. Shin and N. Sebe (1996). A Design Method for Fault-Tolerant Control Systems Based on H_∞ Optimization. *Proc. 35th IEEE CDC*, 1918–1919.

Health & Safety Executive (1995). *Out of Control — Why control systems go wrong and how to prevent failure*, HSE Books.

Henley, E.J. and H. Kumamoto (1992). *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*, IEEE Press.

IEC 61508: Functional safety of electrical/electronic/ programmable electronic safety related systems (1998–2000).

ISO/IEC Guide 51: Guidelines for the inclusion of safety aspects in standards (1990).

ISO/IEC Guide 51 (E): Guidelines for the inclusion of safety aspects in standards (1999). 2nd edition.

Minto, K.D. and R. Ravi (1991). New results on the multi-controller scheme for the reliable control of linear plants. *Proc. 1991 ACC*, 615–619.

Sebe, N. (1996). Diagonal Dominance and Integrity. *Proc. 35th IEEE CDC*, 1904–1909.

Šiljak, D.D. (1995). Decentralized Control and Computations: Status and Prospects. Plenary talk, IFAC Symp. Large Scale Systems: Theory and Applications.

Smith, D.J. (1997). *Reliability, Maintenability and Risk: Practical Methods for Engineers*, 5th edition, Butterworth Heinemann.

Suyama, K. (1997). A New Type Reliable Control System Using Decision by Majority. *Proc. 1997 ACC*, 52–56.

Suyama, K. (1998). Fault Detection of Redundant Sensors Used in Reliable Sampled-Data Control Systems. *Proc. 37th IEEE CDC*, 1161–1164.

Suyama, K. (1999). Functional safety analysis of reliable control systems using decision by majority. *Proc. 1999 ACC*, 618–621.

Suyama, K. and G. Apostolakis (2000). A new direction of reliable control: a context-based approach. *Proc. 2000 ACC*, 352–358.

Suyama, K. and G. Apostolakis (2001). A context-based approach to reliable control: context-dependent performance. *Proc. 2001 ACC*, 1027–1034.

Suyama, K. (2001). Context-based reliable control. *Proc. ECC*, 1273–1278.

Veillette, R.J., J.V. Medanić and W.R. Perkins (1992). Design of Reliable Control Systems. *IEEE Trans. Automat. Contr.*, **37**, 290–304.

Veillette, R.J. (1995). Reliable linear-quadratic state feedback control. *Automatica*, **31**, 137–143.

Vidyasagar, M. and N. Viswanadham (1985). Reliable Stabilization Using a Multi-controller Configuration. *Automatica*, **21**, 599–602.

Yang, G.H., J. Lam and J. Wang (1998). Reliable H_∞ Control for Affine Nonlinear Systems. *IEEE Trans. Automat. Contr.*, **43**, 1112–1117.