

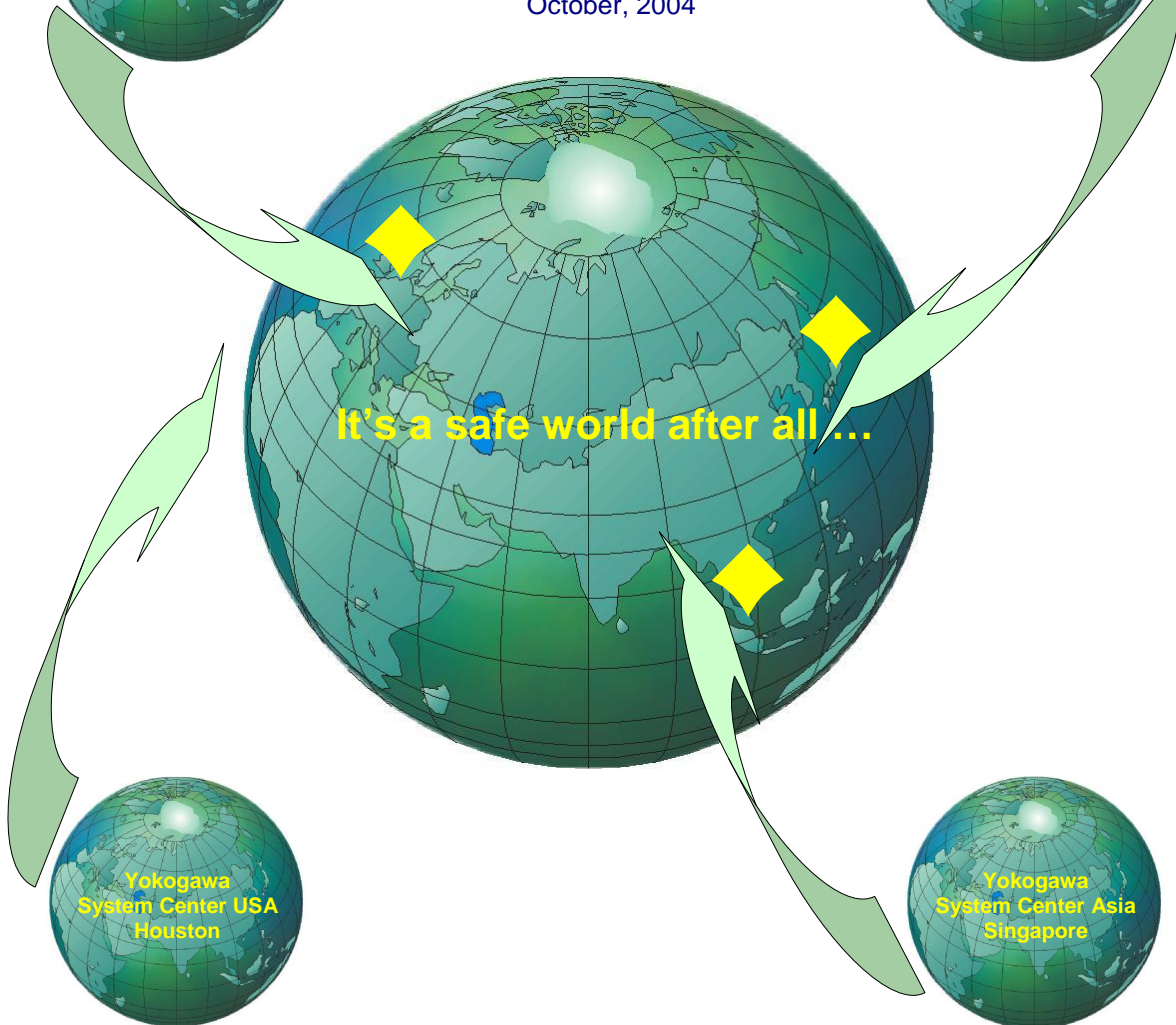
Eliminating the Unexpected - 9

## Reliability with respect to Safety Instrumented Systems

by

**Bonne Hoekstra**

Yokogawa Global Safety Solutions Center  
Apeldoorn, The Netherlands  
October, 2004



# Reliability with respect to Safety Instrumented Systems

by

**Bonne Hoekstra**

Yokogawa Global Safety Solutions Center  
Apeldoorn, The Netherlands  
October, 2004

This paper was published in *Epigram* Spring 2002

## About the author

Bonne Hoekstra is manager of the group Safety Assurance & Consultancy of Yokogawa's Global Safety Solutions Center (located at Yokogawa System Center Europe, Apeldoorn, The Netherlands). He is responsible for independent safety assessments and for the implementation and maintenance of the Functional Safety Management system in Yokogawa's affiliates that realize safety related systems. He is member of the international committees IEC 61508 and 61511. He has over 10 years of experience in the field of functional safety

About the author..... 2

Table of contents..... 3

Definitions, abbreviations and acronyms ..... 4

1 Introduction ..... 5

2 Safety integrity and availability..... 6

3 Literature ..... 9

$\lambda_S$	:	Rate of Safe failures (1/t)
$\lambda_D$	:	Rate of Dangerous failures (1/t)
$\lambda_{Sd}$	:	Rate of Safe failures, detected (1/t)
$\lambda_{Su}$	:	Rate of Safe failures, undetected (1/t)
$\lambda_{Dd}$	:	Rate of Dangerous failures, detected (1/t)
$\lambda_{Du}$	:	Rate of Dangerous undetected failures (1/t)
ESD	:	Emergency Shut Down
Fault-tolerant	:	A SIS or part of a SIS is considered as being fault-tolerant, if it continues to perform its safety functions in spite of the presence of one (or more) dangerous failures.
FMEA	:	Failure Mode Effect Analysis
FSM	:	Functional Safety Management
GRC	:	General Reliability Configurator (Yokogawa's tool for reliability calculations)
HIP(P)S	:	High Integrity (Pressure) Protection System
IEC	:	International Electrotechnical Commission
IEC 61508	:	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61511	:	Functional safety- Safety instrumented systems for the process industry sector
$PFD_{AVG}$	:	Average Probability of Failure on Demand
PLC	:	Programmable Logic Solver
ProSafe-PLC <sup>®</sup>	:	Yokogawa's brand for safety PLC
SFF	:	Safe Failure Fraction: $SFF = (\lambda_S + \lambda_{Dd}) / (\lambda_S + \lambda_{Dd} + \lambda_{Du})$
SIF	:	Safety Instrumented Function
SIL	:	Safety Integrity Level
SIS	:	Safety Instrumented System
SRS	:	Safety Requirements Specification
TMR	:	Triple Modular Redundant

The term Safety Instrumented System (SIS) has been introduced in the international standard IEC 61511 and covers the equipment from sensors, logic solver and final elements that is needed to realise the Safety Integrity Functions (SIF), another IEC term. Reliability with respect to these systems is defined by its ability to command an output to a safe state on a process demand and to function within a required time span without causing a spurious action (e.g. nuisance process trip). The first term has to do with safety integrity as meant by IEC 61508; the second is often presented as process availability, in short availability. The latter is not formally defined in international standards.

IEC 61508 part 2, § 7.4.3.2.1 prescribes: “The probability of failure of each safety function due to random hardware failures, estimated according to 7.4.3.2.2 and 7.4.3.2.3, shall be equal to or less than the target failure measure as specified in the safety requirements specification (see 7.2.3.2).” And adds in note 3: “In order to demonstrate that this has been achieved it is necessary to carry out a reliability prediction for the relevant safety function using an appropriate technique (see 7.4.3.2.2) and compare the result to the target failure measure of the safety integrity requirement for the relevant safety function (see IEC 61508-1, Tables 2 and 3)”.

Systematic failures as well as the human factor are also mentioned in this standard, however they will not be considered in this context for the sake of clearness.

Both can be demonstrated by calculation, both calculations need the failure rates of components involved as input parameter. Be aware that literature mentions a lot of databases with huge deviation in output. A so-called Failure Mode Effect Analysis and/or reliable field experience failure figures are needed to split up the total failure rate of components ( $\lambda$ ) into a safe ( $\lambda_s$ ) and dangerous ( $\lambda_D$ ) fractions (figure 1).

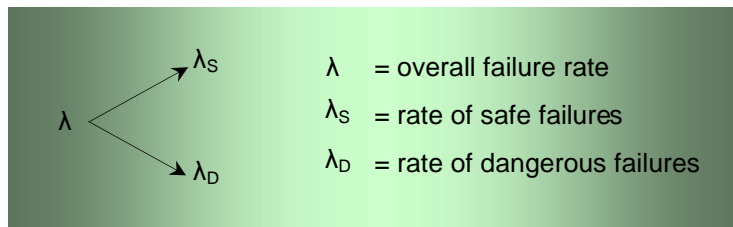


Fig. 1 - Division in safe and dangerous failure rates

The main goal for designing inherent fail safe systems is the reduction of  $\lambda_D$ , without using any additional test circuitry. But in general additional diagnostics will be required to make failures manifest. Therefore it is necessary to make a further division of the failure rates. This is shown in figure 2.

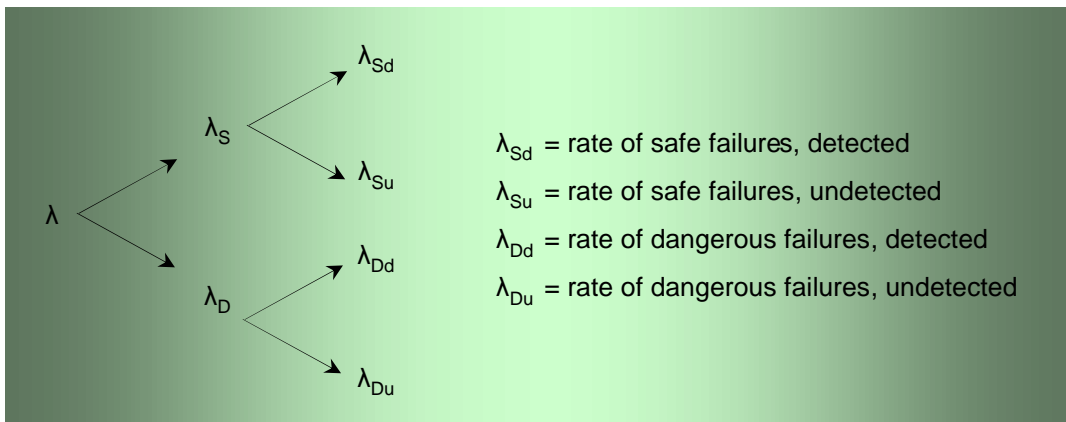


Fig. 2 - Division in safe and dangerous failure rates, diagnostics included

$\lambda_D$  in fig. 2 is split up in a detected (revealed) part ( $\lambda_{Dd}$ ) and an undetected (unrevealed) part ( $\lambda_{Du}$ ). The relation between gives the so-called diagnostic coverage factor (DC):

$$\lambda_{Du} = (1-DC) \times \lambda_D \quad [\text{ref. IEC 61508-2, C1f}]$$

Assuming that detected (revealed) failures can be considered as safe, only  $\lambda_{Du}$  can lead to unsafe action. IEC introduced - with respect to this subject - the factor Safe Failure Fraction to define the required hardware fault tolerance [ref. IEC 61508-2 Table 2 and 3]. The formula is as follows:

$$SFF = (\lambda_{Sd} + \lambda_{Su} + \lambda_{Dd}) / \lambda \quad [\text{ref. IEC 61508-2, C1g}]$$

$\lambda_{Du}$  is used to calculate the PFD: the Probability of Failure on Demand, i.e. the chance that the safety system will miss the ability to command the output to a safe state in case there is a demand from the process".  $\lambda_{Sd}$ ,  $\lambda_{Su}$  and  $\lambda_{Dd}$  can cause a before mentioned spurious action and therefore the sum of these fractions can be used to calculate the process availability.

Table 1 below shows the various system architectures for ESD-applications with the applicable formulas for calculating the PFD. The formulas in this table are meant to calculate the PFD loop based, i.e. for each defined Safety Integrity Function. SIFs have to be laid down in the so-called Safety Requirements Specification (SRS).

safety architecture	name	shortened definition (source: IEC 61508)	block diagram (source: IEC 61508)	trip input	logic relation for de-energized -to -trip configuration	PFD <sub>AVG</sub> (excl. PC and b)	PFD <sub>AVG</sub> (excl. PC, incl. b)
1oo1	one out of one	demand or failing element commands output to a safe state		command to safe state	"0"	$1/2x(\lambda_{Du}xT)$	$1/2x(\lambda_{Du}xT)$
1oo1	one out of one, inherent Fail Safe	demand or failing element commands output to a safe state		command to safe state	"0"	$\lambda_DxMTTR$	$\lambda_DxMTTR$
1oo2	one out of two	one demand or one failing element commands output to a safe state		command to safe state	"0"	$1/3x(\lambda_{Du}xT)^2$	$1/3x((1-\beta)x\lambda_{Du}xT)^2 + 1/2x\beta x\lambda_{Du}xT$
1oo2D	one out of two, with diagnostics	one demand or simultaneous failing elements command output to a safe state		command to safe state	"0"	$1/3x(\lambda_{Du}xT)^2$	$1/3x((1-\beta)x\lambda_{Du}xT)^2 + 1/2x\beta x\lambda_{Du}xT$
1oo3	one out of three	either demand or failing element commands a output to a safe state		command to safe state	"0"	$1/4(\lambda_{Du}xT)^3$	$1/4x((1-\beta)x\lambda_{Du}xT)^3 + 1/2x\beta x\lambda_{Du}xT$
2oo2	two out of two	two demands or simultaneous failing elements command output to a safe state		command to safe state	"0"	$\lambda_{Du}xT$	$(1-\beta)x\lambda_{Du}xT + 1/2x\beta x\lambda_{Du}xT$
2oo3	two out of three	two demands or two failing elements command output to a safe state		command to safe state	"0"	$(\lambda_{Du}xT)^2$	$((1-\beta)x\lambda_{Du}xT)^2 + 1/2x\beta x\lambda_{Du}xT$

Table 1 - Single and multiple architectures of Safety Instrumented Systems

The (approximate) formulas in this table calculate the average PFD over the period T (proof test period). The other symbols used in this table mean:

**MTTR** = Mean Time To Repair  
 **$\beta$**  = Common cause factor  
**PC** = proof test coverage factor

The relation between PFD and Safety Integrity Level (SIL) is shown in table 2. The Risk Reduction Factor is the reciprocal value of the PFD

Safety Integrity Level (SIL)	Average Probability of Failure on Demand PFD <sub>AVG</sub>	Risk Reduction Factor
4	$\geq 10^{-5}$ to $< 10^{-4}$	> 10 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	1 000 - 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	100 - 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	10 - 100
0	Control (N/A)	

Source: IEC 61508-1 Table 2

Table 2 - Relation between SIL and PFD<sub>AVG</sub>

Yokogawa apply the ProSafe-SLS<sup>®</sup>, a discrete logic system based on the core-transistor-logic principle, in 1oo1 configuration (inherent fail-safe) to realize HIP(P)S (High Integrity (Pressure) Protection System) with SIL 4 requirements. This system combines its highest safety integrity to a high process availability level (over 99.99%) due to its simplicity. Figures can be proved by over thirty years of experience.

ProSafe-PLC<sup>®</sup> is a PLC-based system that can be applied in single and multiple configurations. In the so-called 1oo2D configuration (D for Diagnostics) this system can be applied in SIL 3 safety loops. As for the process availability this system can be seen as full redundant. Availability figures of far over 99.99 % can be reached, due to its high common cause strength. This performance can be compared with that of Triple Modular Redundant (TMR) architectures as described in the summer 2001 edition of Epigram. Table 1 shows that with low beta factor (common cause) the PFD-figure of a 1oo2D configuration is even three times better than that of a TMR (2oo3 configuration).

To demonstrate that the safety systems to be delivered meet the reliability targets, Yokogawa have developed the formula based calculation tool GRC (General Reliability Configurator) and has let develop by the Eindhoven (NL) University a Markov-model based tool with both numeric and graphical output.

- [1] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. - IEC, 1998-2000.
- [2] IEC 61511: Functional safety – Safety instrumented systems for the process industry sector. - IEC, 2003.
- [3] R. Tiezema: Common-Cause Effects on Safety Related PLC's – YIS-013, 2<sup>nd</sup> Edition September 1999.
- [4] Goble, William M. and Fialkowsky, Charles M.: Building Safer Protection Systems with High Common Cause Strength. ISA Symposium, Cleveland, June 1996

**Global Safety Solutions Center**

YOKOGAWA SYSTEM CENTER EUROPE B.V.  
Lange Amerikaweg 55  
7332 BP Apeldoorn  
P.O.BOX 20020  
7302 HA Apeldoorn  
The Netherlands

Tel.: +31-55-5389-500  
Fax: +31-55-5389-510  
E-mail: [info@nl.yokogawa.com](mailto:info@nl.yokogawa.com)  
[www.yokogawa-europe.com](http://www.yokogawa-europe.com)

**Yokogawa System Center USA**

YOKOGAWA CORPORATION OF AMERICA  
5010 Wright Road  
Suite 100  
Stafford TX 77477  
United States of America

Tel.: +1-281-340-3900  
Fax: +1-281-340-3939  
E-mail: [info@yca.com](mailto:info@yca.com)  
[www.yca.com](http://www.yca.com)

**Yokogawa System Center Asia**

YOKOGAWA ENGINEERING ASIA Pte. Ltd.  
5 Bedok South Road  
Singapore 469270

Tel.: +65-6241-9933  
Fax: +65-6241-9573  
E-mail: [info@sg.yokogawa.com](mailto:info@sg.yokogawa.com)  
[www.yokogawa.com/sg](http://www.yokogawa.com/sg)

- ✦ All the brands or names of Yokogawa Electric's products used in this booklet are either trademarks or registered trademarks of Yokogawa Electric.
- ✦ All other company and product names mentioned in this booklet are trade names, trademarks or registered trademarks of their respective companies.

YOKOGAWA ELECTRIC CORPORATION  
World Headquarters  
9-32, Nakacho 2-chome, Musashino-shi, Tokyo 180-8750, JAPAN

Subject to change without notice  
Copyright © 2004 Yokogawa System Center Europe B.V.  
Source file:EtU-9 Reliability with respect to SIS, Revision : HSA041013