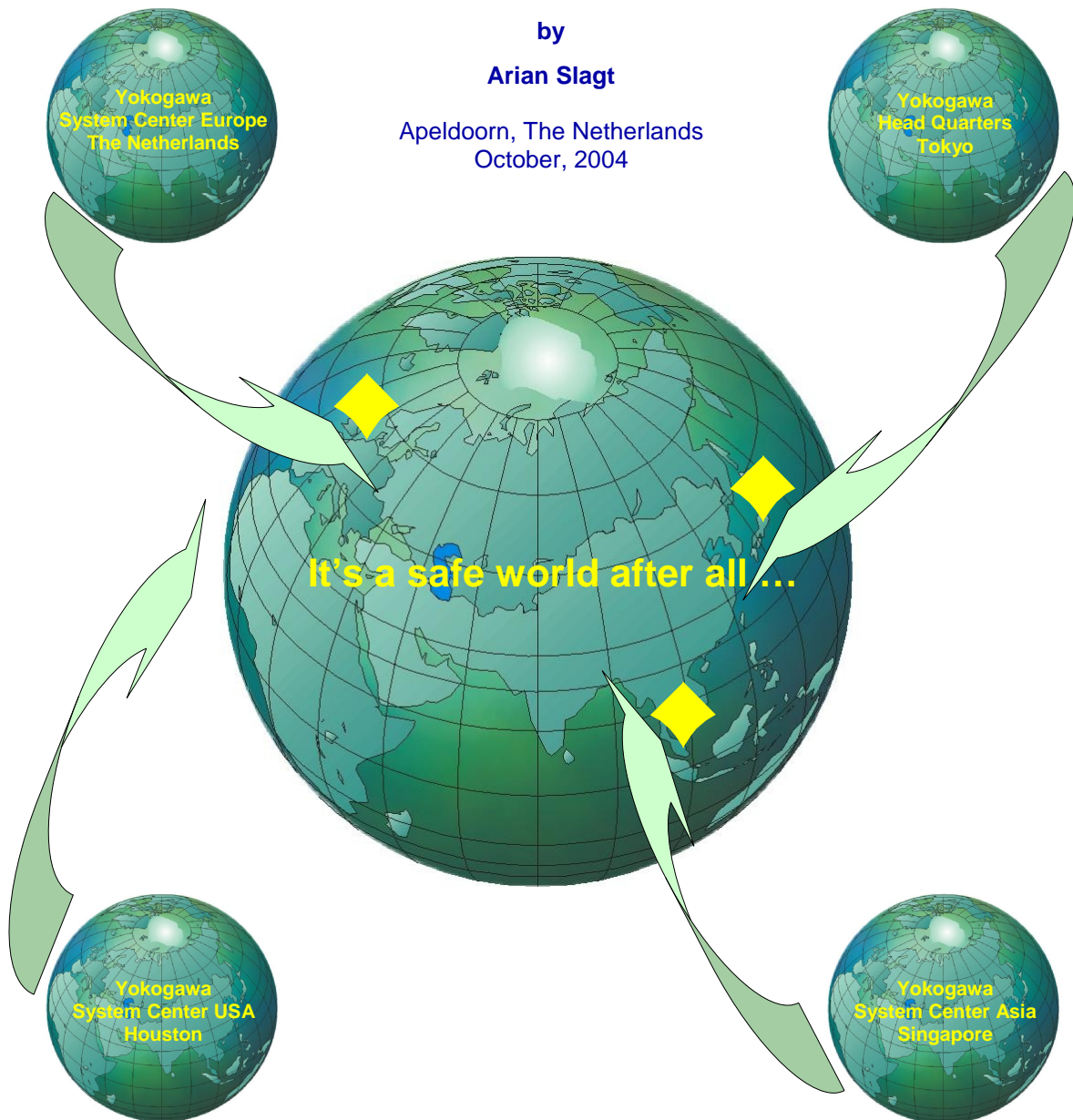


Eliminating the Unexpected - 15

## TO BE CERTIFIED OR NOT?

by  
Arian Slagt

Apeldoorn, The Netherlands  
October, 2004



# To BE CERTIFIED OR NOT?

by

**Arian Slagt**

Apeldoorn, The Netherlands  
October, 2004

## Disclaimer

*This document was written in accordance with established regulations and standards of technology. Yokogawa SCE accepts no responsibility for the correctness of the regulations or standards on which this document is based. The use of this document to establish Safety Instrumented Functions does not relieve the user from any of his responsibility to establish procedures sufficient to ensure the safety of his operations or to meet legal obligations. Yokogawa SCE will accept no liability for correctness or completeness of this document. In particular, Yokogawa SCE does not guarantee the design of facilities or choice of products used when the user uses this document or any resulting modification of this document.*

*Yokogawa SCE's guarantee is restricted to the correction of errors or deficiencies reported by the purchaser within a reasonable period of time. Under no circumstances shall Yokogawa SCE be obligated to any amount beyond the purchase price of the document.*

## About the author

*Arian Slagt, functional safety expert for Yokogawa Europe, looks at safety certification and the proven-in-use procedure for instrumentation in the hydrocarbon industry.*

*This article has been published in "Hydrocarbon Engineering", September 2004.*

## Table of contents

About the author.....	2
Table of contents.....	2
To be Safety Certified or not ... that's the question .....	3
Introduction.....	3
Certification .....	3
Proven-in-use .....	4
Case study .....	5
Conclusion.....	5

**Introduction**

When considering functional safety in the hydrocarbon industry, there are two key standards: IEC 61508, the generic framework for functional safety, and IEC 61511, the specific standard for the process industry. The IEC 61511 standard allows use of instruments in safety functions based either on compliance with the IEC 61508 standard or based on prior-use (also called proven-in-use). Compliance to the IEC 61508 standard normally has to be verified by an independent certifying body, hence is referred to as 'certified'. A key European certification body is TÜV in Germany.

Within the instrumentation and control fraternity the debate has started - what is better? Proven-in-use or certified field instruments? Some end-users will only accept an instrument when it is certificated, while other companies have a very strong preference towards proven-in-use instruments. In this article we will review both methods of assessment, consider the advantages of each and check the factors that must be taken into account when selecting instruments.

**Certification**

When an instrument is defined as certified it should meet two criteria:  
 The instrument is designed and manufactured according to a predefined standard e.g. IEC 61508  
 The conformance has been verified and approved by an independent certification body.  
 The IEC 61508 standard has detailed requirements pertaining to design process, hardware design, software design, and production processes. All these aspects must be taken into account by the manufacturer and reviewed by the certifying body.

When judging a certificate, the user must consider in detail. Certificates are sometimes limited to the hardware Failure Mode and Effect Analysis (FMEA) only. From the FMEA the so-called Safe Failure Fraction (SFF) can be determined. This value is very important as it defines the minimum number of devices that must be applied in a safety loop when applying the IEC 61508 standard. See Table 1 for the details. For full compliance with the standard the other requirements should be included appropriately.

		Number of devices		
		SIL1	SIL2	SIL3
IEC 61508	SFF			
	60 – 90%	1	2	3
	90 – 99%	1	1	2
IEC 61511	Standard	1	2	3
	Prior-use	1	1	2

Table 1: Minimum number of devices depending on the Safety Integrity Level (SIL).

Often the Safety Integrity Level (SIL) is printed boldly on an instrument's certificate, but a SIL can only be claimed by a complete safety function, not by a single device. A more important parameter of a device is its dangerous undetected failure rate (Fdu). From this Fdu every body can calculate himself the partial

contribution to the probability of failure on demand (PFD) of the loop, depending on the used proof test interval and other parameters.

Another consideration is the certifying body. Is this a well-known and accepted company? There is always a report detailing performance and testing that resulted in a device gaining its certificate. The end-user must read this report to understand the performance of the device fully and the limitations of the certification.

## Proven-in-use

Proven-in-use means that a number of that device has been used satisfactorily over a defined period of time, in a certain application. Proven-in-use information is important as it defines the minimum number of devices that must be applied in a safety loop when applying the IEC 61511 standard. When a device can be justified to be proven-in-use, the minimum number of devices in a safety loop can be reduced by one, compared to ordinary devices. (See Table 1 for details.)

It is not easy to claim proven-in-use. According to the standard, many necessary elements of performance must be taken into account. For field devices these include:

- Consideration of the manufacturer's production quality system
- Adequate identification and specification of the device
- Demonstration of the performance in similar application and environments
- The volume of operating experience
- Unused features must be identified and it must be unlikely that they jeopardize the safety function.
- For SIL3 applications a formal assessment of the field device must be carried out.

The standard does not specify in detail how to do all the above. For instance it does not prescribe a minimum number of devices and a minimum time of usage to claim the correct volume of experience. This makes it challenging, or very easy to claim proven-in-use, dependant upon the device. Buyers beware.

When an end-user or a manufacturer claims proven-in-use for a certain field device, the arguments must be analysed carefully to understand the basis of the claim. A report from an independent certifying body may help to give confidence to the end-user, too. For a proven-in-use device the failure rate must be known in order to be able to calculate the achieved PFD. That means an FMEDA must be executed to find the failure rates. This data should preferably be checked by an independent organization, so a certificate is still needed.

Some companies maintain an internal list with failure rates based on their own experience. For MTBF figures this data might be acceptable. For the value of the "undetected dangerous failure rate" (Fdu), obtaining the right information is very difficult due to its very low value. To prove the low Fdu (e.g. 1.00E-8/hr) requires a very high number (n) of transmitters under operation/test during a very long period of time (T). In practice, the requirements for T and n are very difficult to fulfil. In addition, there will be a number of modifications during T and, moreover, different devices operate under the different environmental conditions.

End-users have to document carefully if a failure is safe or undetected and dangerous. Undetected dangerous failures are found only during proof testing or as cause of an accident. Therefore suppliers as well as users will meet frequent filing and logging problems to obtain valid results. More information can be found in a publication of the German "Arbeitsschutz", written by TÜV Rheinland: *Betriebsbewahrung von Hard- und Software beim Einsatz von Rechnern für Sicherheitsaufgaben*. (Translates as: *Proven in use of hard- and software of computers in safety applications*).

## Case study

When Yokogawa began a redesign of its EJA pressure transmitter, it was decided to follow the IEC 61508 rules. At the start of the project a development plan for the extensions was prepared. The German TÜV was involved throughout the development as an independent certification body to verify that all steps from IEC 61508 had been followed. Both the hardware design and the software design were executed in line with IEC 61508.

As part of the hardware evaluation an FMEDA has been executed to arrive at the failure fractions. At the beginning of 2004 TÜV released the certificate for the EJX transmitter, which demonstrates full compliance to the IEC 61508 standard.

The EJX is based on the EJA transmitter. More than a million of these are in use worldwide, in a wide range of applications and environments. Software releases during the life of the transmitter have been carefully documented and administrated, which is verified by TÜV. By continuing the evolution of the EJ-series of transmitter Yokogawa has combined best of both worlds: an IEC 61508 certified instrument with a proven track record.



## Conclusion

Both certification and proven-in-use are good in principle. However, the real value depends on the limiting conditions of the assessment and the way that these are described to and understood by the end-user. Both methods are also complementary: it is hard to develop new devices that are proven-in-use when introduced, but technical innovation is impossible when only proven-in-use would be accepted.

**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-15 To be certified or not 041209, Revision : HSA041209