The Use of 3rd Party
in the sense of Functional Safety

Dr. Thorsten Gantevoort
Head of Certification Body, TUV Rheinland

Safety Case
Symposium 2018
Singapore

Functional Safety and Cyber Security @ TÜV Rheinland

Business Area: Automation, Functional Safety and Security
Accredited as Certification Body, Test Lab and Inspection Body

Products	Systems	Applications	Qualification
Test and Certification	Functional Safety Management & Security Life-Cycle	Application and System Implementation	Trainings and Workshops

FS & Cyber Security

Application Areas:
Machinery, Oil & Gas, Process Industry, Automotive, Power Plants etc.

Third Party

How is 3rd Party commonly defined?

https://en.wiktionary.org

Someone not directly involved in a transaction. A third entity in the Seller (first party) and Customer (second party) relationship.

Someone only incidentally or tangentially connected to an incident or dispute; someone other than the principals; a bystander or independent witness.

A political party in opposition to the main parties in a two-party system

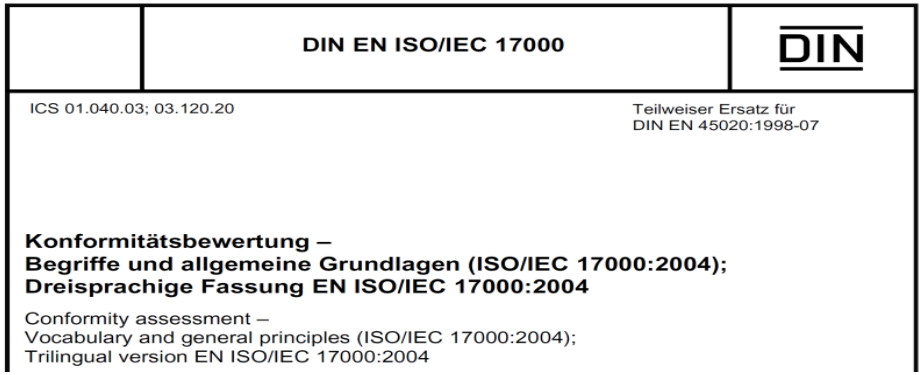
https://en.wikipedia.org/wiki/Independent_test_organization

An independent test organization is an organization, person, or company that tests products, materials, software, etc. according to agreed requirements. The test organization can be affiliated with the government or universities or can be an independent testing laboratory. They are independent because they are not affiliated with the producer nor the user of the item being tested: no commercial bias is present. These “contract testing" facilities are sometimes called "third party" testing or evaluation facilities.

Third Party

ISO/IEC 17000:2004

- **first-party conformity assessment activity**
  conformity assessment activity that is performed by the person or organization that provides the object
- **second-party conformity assessment activity**
  conformity assessment activity that is performed by a person or organization that has a user interest in the object
- **third-party conformity assessment activity**
  conformity assessment activity that is performed by a person or body that is independent of the person or organization that provides the object and of user interests in that object
- **conformity assessment**
  demonstration that specified requirements relating to a product, process, system, person or body are fulfilled
  - NOTE 1 The subject field of conformity assessment includes activities defined elsewhere in this International Standard, such as testing, inspection and certification, as well as the accreditation of conformity assessment bodies.



DIN EN ISO/IEC 17000

DIN

ICS 01.040.03; 03.120.20

Teilweiser Ersatz für
DIN EN 45020:1998-07

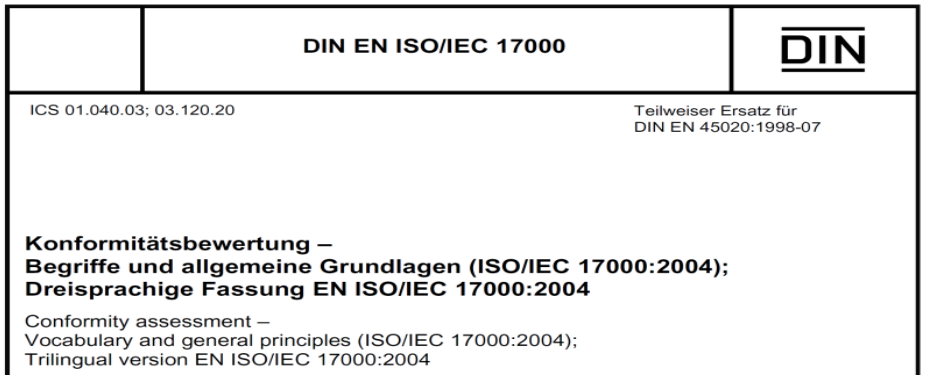
Konformitätsbewertung –
Begriffe und allgemeine Grundlagen (ISO/IEC 17000:2004);
Dreisprachige Fassung EN ISO/IEC 17000:2004

Conformity assessment –
Vocabulary and general principles (ISO/IEC 17000:2004);
Trilingual version EN ISO/IEC 17000:2004

Attestations of parties

ISO/IEC 17000:2004

- **Attestation**
  issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated
- **Declaration**
  first-party attestation
- **Certification**
  third-party attestation related to products, processes, systems or persons
- **Accreditation**
  third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks



DIN EN ISO/IEC 17000

DIN

ICS 01.040.03; 03.120.20

Teilweiser Ersatz für
DIN EN 45020:1998-07

Konformitätsbewertung –
Begriffe und allgemeine Grundlagen (ISO/IEC 17000:2004);
Dreisprachige Fassung EN ISO/IEC 17000:2004

Conformity assessment –
Vocabulary and general principles (ISO/IEC 17000:2004);
Trilingual version EN ISO/IEC 17000:2004

Accreditations of parties

Example: Accreditation as Certification Body

DAkkS Deutsche Akkreditierungsstelle

Deutsche Akkreditierungsstelle GmbH

Beliehene gemäß § 8 Absatz 1 AkkStelleG i.V.m. § 1 Absatz 1 AkkStelleGBV
Unterzeichnerin der Multilateralen Abkommen
von EA, ILAC und IAF zur gegenseitigen Anerkennung

Akkreditierung

Die Deutsche Akkreditierungsstelle GmbH bestätigt hiermit, dass die Zertifizierungsstelle

TÜV Rheinland Industrie Service GmbH
Zertifizierungsstelle Energiesysteme, Renewables, Grid & Automation
Am Grauen Stein 27, 51105 Köln

die Kompetenz nach DIN EN ISO/IEC 17065:2013 besitzt, Zertifizierungen von Produkten, Prozessen und Dienstleistungen in folgenden Bereichen durchzuführen:

On- und Offshore Windenergieanlagen und deren Komponenten;
Netzintegration von Erzeugungseinheiten und Anlagen einschließlich Komponenten und deren Kommunikation;
Systemdienstleistungen bei dezentralen Erzeugungseinheiten und Anlagen einschließlich Komponenten;
Funktional sichere Produkte, Anwendungen und Systeme einschließlich Functional Safety Management;
Security

Die Akkreditierungsurkunde gilt nur in Verbindung mit dem Bescheid vom 12.02.2016 mit der Akkreditierungsnummer D-ZE-11052-02 und ist gültig bis 02.09.2017. Sie besteht aus diesem Deckblatt, der Rückseite des Deckblatts und der folgenden Anlage mit insgesamt 27 Seiten.

Registrierungsnummer der Urkunde: **D-ZE-11052-02-00**

Berlin, 12.02.2016

Im Auftrag Dr. Heike Manke
Abteilungsleiterin

Die Deutsche Akkreditierungsstelle GmbH bestätigt hiermit, dass die Zertifizierungsstelle

TÜV Rheinland Industrie Service GmbH

Zertifizierungsstelle Energiesysteme, Renewables, Grid & Automation, Am Grauen Stein 27, 51105 Köln

die Kompetenz nach DIN EN ISO/IEC 17065:2013 besitzt, Zertifizierungen von Produkten, Prozessen und Dienstleistungen in folgenden Bereichen durchzuführen:

On- und Offshore Windenergieanlagen und deren Komponenten;

Netzintegration von Erzeugungseinheiten und Anlagen einschließlich Komponenten und deren Kommunikation;

Systemdienstleistungen bei dezentralen Erzeugungseinheiten und Anlagen einschließlich Komponenten;

Funktional sichere Produkte, Anwendungen und Systeme einschließlich Functional Safety Management; Security

Accreditations - Scope

Example: Accreditation as Certification Body

Scope (translated):

Functional safe products, applications and systems including
Functional Safety management;
Security

? … but to which standards and regulations?

DAkkS Deutsche Akkreditierungsstelle

Deutsche Akkreditierungsstelle GmbH

Anlage zur Akkreditierungsurkunde D-ZE-11052-02-00
nach DIN EN ISO/IEC 17065:2013

Gültigkeitsdauer: 12.02.2016 bis 02.09.2017 Ausstellungsdatum: 12.02.2016

Urkundeninhaber:

TÜV Rheinland Industrie Service GmbH
Zertifizierungsstelle Energiesysteme, Renewables, Grid & Automation
Am Grauen Stein 27, 51105 Köln

Zertifizierungen von Produkten in den Bereichen:

On- und Offshore Windenergieanlagen und deren Komponenten;
Netzintegration von Erzeugungseinheiten und Anlagen einschließlich Komponenten und deren Kommunikation;
Systemdienstleistungen bei dezentralen Erzeugungseinheiten und Anlagen einschließlich Komponenten;
Funktional sichere Produkte, Anwendungen und Systeme einschließlich Functional Safety Management;
Security

verwendete Abkürzungen: siehe letzte Seite

1 On- und Offshore Windenergieanlagen und deren Komponenten

IEC 61400-22 2010-05	Wind turbines - Part 22: Conformity testing and certification
QMA 3.120.01 2012-02	Durchführung von Prüfungen und Zertifizierungen von Windenergieanlagen

Adobe Acrobat Document

Seite 1 von 27

Safety Case Symposium 2018 Singapore

Accreditation

Benefits

For companies

- Better acceptance of products and services eases market access or makes it possible
- Tested once, accepted everywhere: International comparability and recognition […]
- Proof of competence facilitates the selection of a suitable service provider for the conformity assessment of goods and services

For accredited bodies

- Objective proof of quality and competence for the activities of conformity assessment bodies according to international standards
- Competitive advantages over non-accredited market participants

For consumers

- more consumer trust in the quality of products and services - notwithstanding a complex global market
- fewer production errors or recalls

For legislators

- flexible alternative to legislation

Source: www.dakks.de
DAkkS is the national accreditation body for Germany.

Requirements from Regulations and Standards

IEC 61511:2016 (IEC 61508:2010)

- **independent organization**
  organization that is separate and distinct, by management and other resources, from the organizations responsible for the activities that take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation
- **independent person**
  person who is separate and distinct from the activities which take place during the specific phase of the SIS safety life-cycle that is subject to the FSA or validation and does not have direct responsibility for those activities

Minimum level of independence (IEC 61508)	SIL / SC			
	1	2	3	4
Independent person	X	X1	Y	Y
Independent department	--	X2	X1	Y
Independent organization	--	--	X2	X

X: minimum
X2 more appropriate than X1
Y: insufficient

Requirements from Regulations and Standards

IEC 61511 (IEC 61508) – FSM Roles and Responsibilities

- Persons, departments or organizations involved in SIS safety life-cycle activities shall be competent to carry out the activities for which they are accountable.
- The following items shall be addressed and documented when considering the competence of persons, departments, organizations or other units involved in SIS safety life-cycle activities:
- a) engineering knowledge, training and experience appropriate to the process application;
- b) …i)
- A procedure shall be in place to manage competence of all those involved in the SIS life cycle. Periodic assessments shall be carried out to document the competence of individuals against the activities they are performing and on change of an individual within a role.

If a supplier makes any functional safety claims for a product or service, which are used by the organization to demonstrate compliance with the requirements of this part of IEC 61511, the supplier shall have a functional safety management system.

Requirements from Regulations and Standards

Machinery Directive – Notified Body

The body, its director and the staff responsible for carrying out the verification tests shall not be the designer, manufacturer, supplier or installer of machines which they inspect, nor the authorised representative of any of these parties. They shall not become involved […]

The body and its staff shall carry out the verification tests with the highest degree of professional integrity and technical competence and shall be free from all pressures and inducements, particularly financial, […]

The staff responsible for inspection shall have:

sound technical and vocational training,

satisfactory knowledge of the requirements of the tests they carry out and adequate experience of such tests,

the ability to draw up the certificates, records and reports required to authenticate the performance of the tests.

[…]

! A Notified Body shall be a third party (independent) and competent

Conclusion

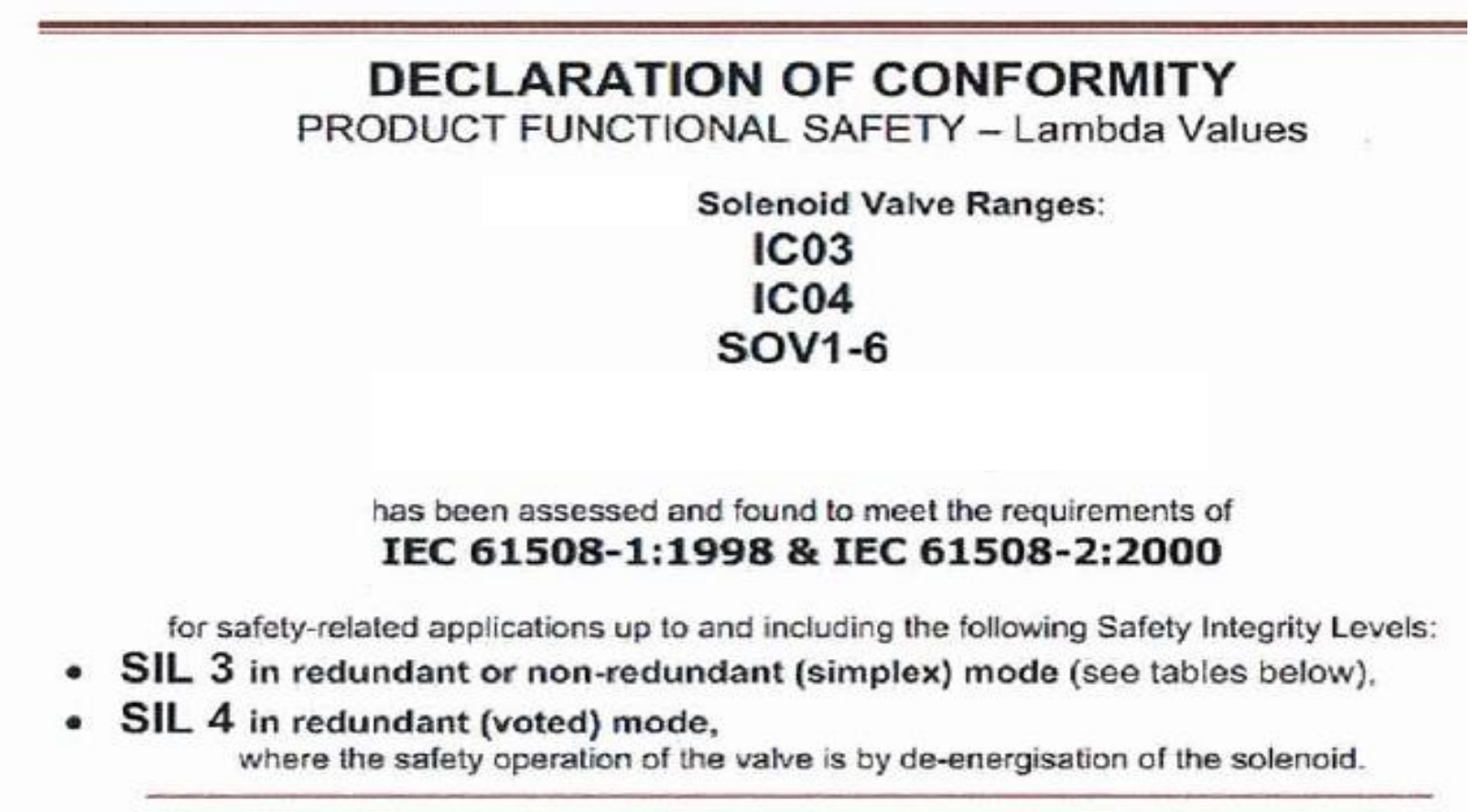
Third Party in the Sense of Functional Safety

- is not only an independent organization
- It is (shall be)
- an independent , credible organization
- an organization being transparent and full of integrity
- an organization with (managed) competencies
- an organization with a Functional Safety Management and
- part of the life cycle/FSM of the “first party”

- Accreditation proofs independence and competence, but is not mandatory
- The “first party” (life cycle phase responsible) is responsible to assess the results of a third party, to demonstrate that the lifecycle *outputs meet in all respect the objectives and the requirements specified for the phase*.

Attestation - Examples

- SIL 4 - Self declaration



DECLARATION OF CONFORMITY

PRODUCT FUNCTIONAL SAFETY – Lambda Values

Solenoid Valve Ranges:

IC03

IC04

SOV1-6

has been assessed and found to meet the requirements of

IEC 61508-1:1998 & IEC 61508-2:2000

for safety-related applications up to and including the following Safety Integrity Levels:

- **SIL 3 in redundant or non-redundant (simplex) mode** (see tables below),
- **SIL 4 in redundant (voted) mode,**
  where the safety operation of the valve is by de-energisation of the solenoid.

Attestation - Examples

SIL 4 (?) - Self declaration

ACTUATOR VALUES :

- $\lambda_{SD} = \lambda_{DD} = 0$ (1/hours)
- $\lambda_{SU} = 7.6586\ E^{-07}$ (1/hours)
- $\lambda_{DU} = 1.1416\ E^{-09}$ (1/hours)
- $\lambda_{TOT} = 7.67\ E^{-07}$ (1/hours)

- $MTBF = \frac{1}{\lambda_{TOT}} = 1.3E^{06}$ (hours)
- SFF=99.9%
- $PFD_G = 5.01E^{-6}$

Attestation - Examples

Fake certificate

Origin, integrity and validity can be checked on https://fs-products.tuvasi.com/

TÜV

TÜV Rheinland Group

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie

ZERTIFIKAT
CERTIFICATE

Nr./No.977/EL 397.00/06

Prüfgegenstand **Product tested**	Theatersteuerung für Punkt- und Prospektzüge sowie Versenkeinrichtungen	**Hersteller** **Manufacturer**	[redacted]
Typbezeichnung **Type designation**	Kinesys Vector V2	**Verwendungs-zweck** **Intended application**	Steuerung von theatertechnischen Einrichtungen
Prüfgrundlagen **Codes and standards forming The basis of testing**	IEC 61508, Teil 1 – 7:2000 DIN 56950:2005-04 BGV C1 – Kapitel V		
Prüfungsergebnis **Test results**	Einsetzbar für die Steuerung von theatertechnischen Einrichtungen. Die Steuerung KINESYS Vector V2 erfüllt die Anforderungen bis einschließlich SIL 3 entsprechend der IEC 61508.		
Prüfungsergebnis **Test results**	Das Kapital "Auflagen/Vor Ort Abnahme" des Prüfberichtes sowie die Auflagen der Bedienungshandbücher sind zu beachten.		

Der Prüfbericht-Nr. 977/EL 397.00/06 vom 2009-02-19 ist Bestandteil dieses Zertifikates. Dieses Zertifikates ist nur gültig für Erzeugnisse, die mit dem Prüfgegen-stand übereinstimmen. Es wird ungültig bei jeglicher Änderung der Prügrundlagen für den angegebenen Verwendungszweck.

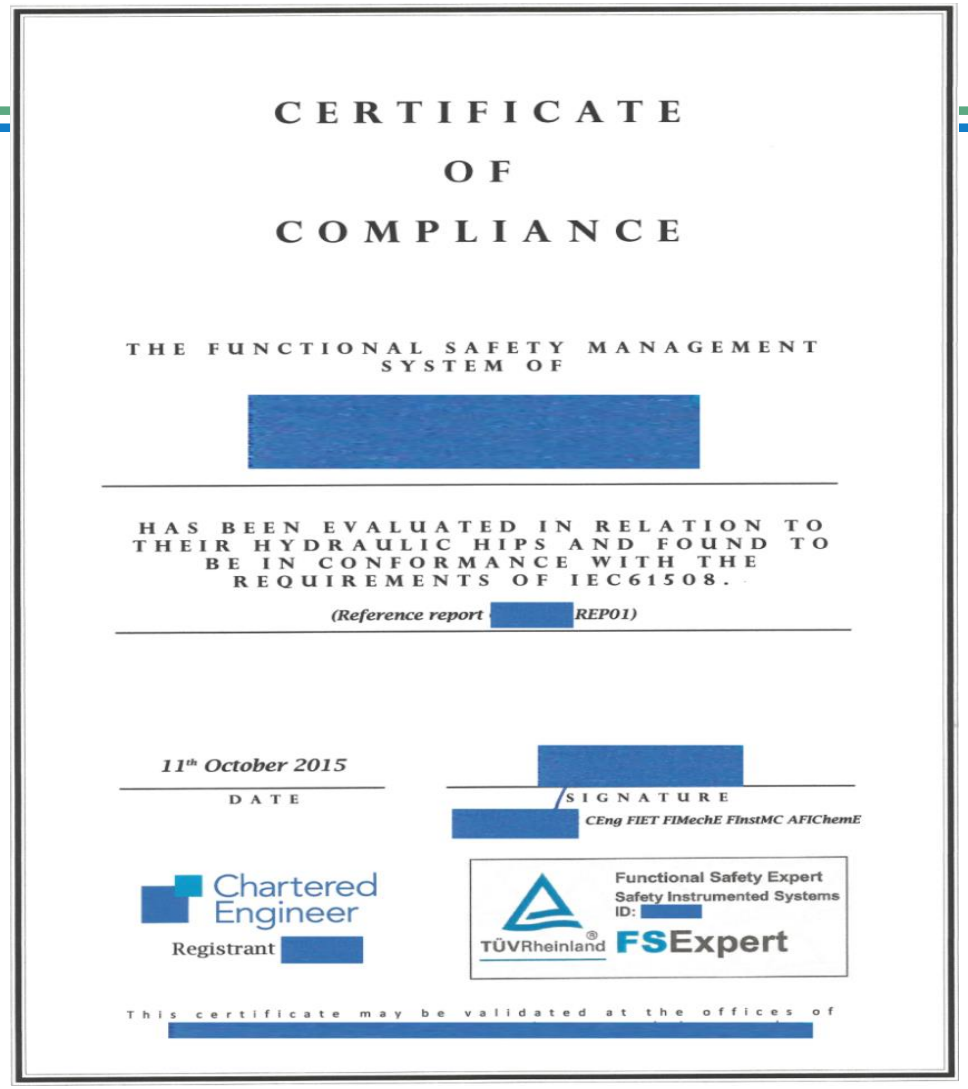
The test report-no 977/EL 397.00/06 vom 2009-02-19 is an integral part of this certificate. This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standard forming the basis of testing for the intended application .

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 00 51, 51101 Köln

2009-02-19
Datum/Date | Firmenstempel / Company seal | Unterschrift/Signature

Attestation - Examples

Misuse of TÜV Logo



CERTIFICATE

OF

COMPLIANCE

THE FUNCTIONAL SAFETY MANAGEMENT SYSTEM OF

[redacted]

HAS BEEN EVALUATED IN RELATION TO THEIR HYDRAULIC HIPS AND FOUND TO BE IN CONFORMANCE WITH THE REQUIREMENTS OF IEC61508.

(Reference report [redacted] REP01)

11th October 2015

DATE

[redacted]

SIGNATURE

[redacted] *CEng FIET FIMechE FInstMC AFIChemE*

Chartered Engineer

Registrant [redacted]

Functional Safety Expert
Safety Instrumented Systems
ID: [redacted]

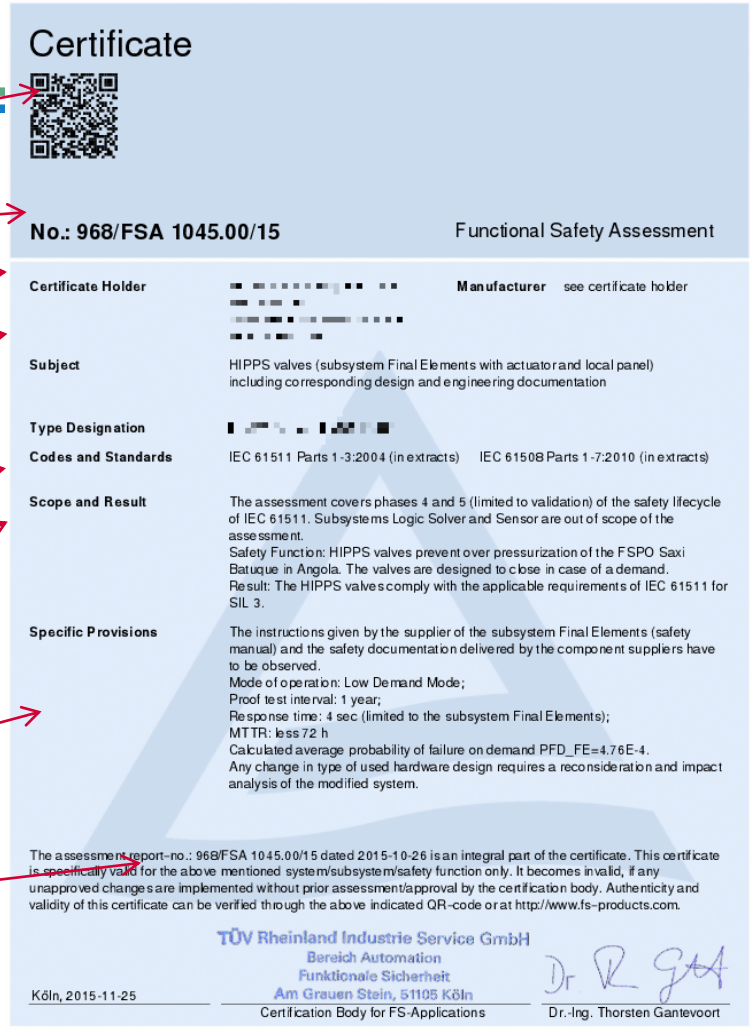
TÜVRheinland® FSExpert

This certificate may be validated at the offices of [redacted]

Attestation

TÜV Rheinland Certificates - Assessments

- Direct Link to certificate in TÜV database
- Unique Certificate No.
- Certificate Holder / Manufacturer
- Subject: states together with type designation the assessed product, system etc.
- Type designation
- Applied codes and standards, i.e. IEC 61508, IEC 61511 (maybe only in extracts)
- Scope and Result: States the explicit scope with all limitations and the results of the assessment
- Specific Provisions: provides restrictions, additional requirements
- Assessment Report with full information



Certificate

No.: 968/FSA 1045.00/15 Functional Safety Assessment

Certificate Holder	[redacted] Manufacturer see certificate holder
Subject	HIPPS valves (subsystem Final Elements with actuator and local panel) including corresponding design and engineering documentation
Type Designation	[redacted]
Codes and Standards	IEC 61511 Parts 1-3:2004 (in extracts) IEC 61508 Parts 1-7:2010 (in extracts)
Scope and Result	The assessment covers phases 4 and 5 (limited to validation) of the safety lifecycle of IEC 61511. Subsystems Logic Solver and Sensor are out of scope of the assessment. Safety Function: HIPPS valves prevent over pressurization of the FSPO Saxi Batuque in Angola. The valves are designed to close in case of a demand. Result: The HIPPS valves comply with the applicable requirements of IEC 61511 for SIL 3.
Specific Provisions	The instructions given by the supplier of the subsystem Final Elements (safety manual) and the safety documentation delivered by the component suppliers have to be observed. Mode of operation: Low Demand Mode; Proof test interval: 1 year; Response time: 4 sec (limited to the subsystem Final Elements); MTTR: less 72 h Calculated average probability of failure on demand PFD_FE=4.76E-4. Any change in type of used hardware design requires a reconsideration and impact analysis of the modified system.

The assessment report-no.: 968/FSA 1045.00/15 dated 2015-10-26 is an integral part of the certificate. This certificate is specifically valid for the above mentioned system/subsystem/safety function only. It becomes invalid, if any unapproved changes are implemented without prior assessment/approval by the certification body. Authenticity and validity of this certificate can be verified through the above indicated QR-code or at http://www.fs-products.com.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2015-11-25 — Certification Body for FS-Applications — Dr.-Ing. Thorsten Gantevoort

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

Safety Case Symposium 2018 Singapore

Attestation

TÜV Rheinland Certificates - FSM

QR-Code: Shows original issued FSM certificate

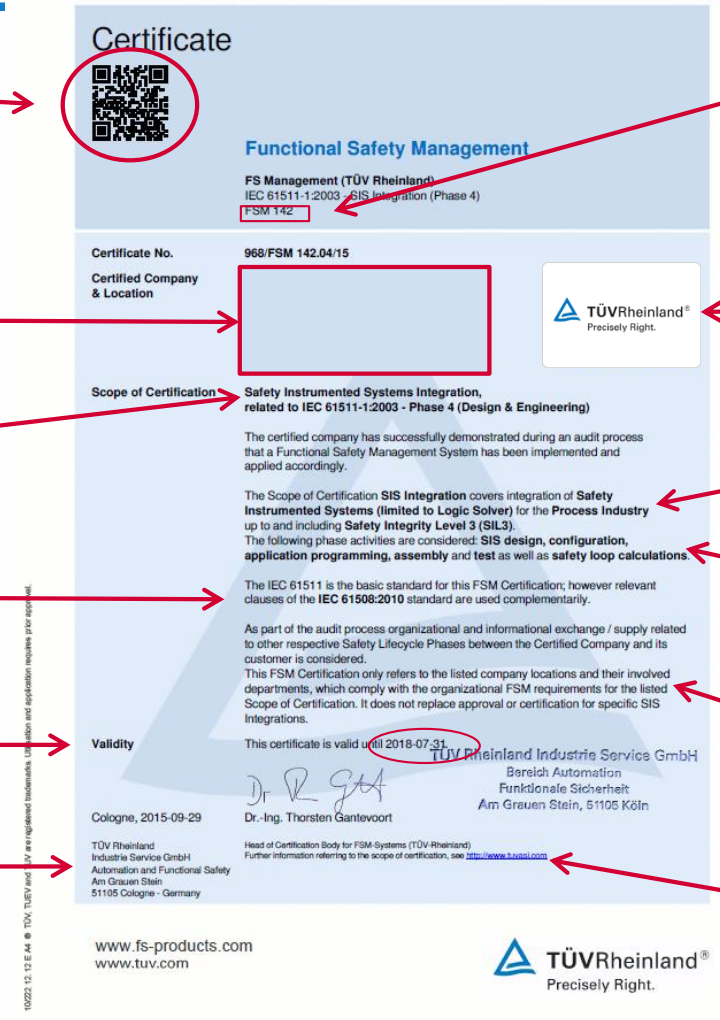
Company Location and legal address

Defined scope and relevant standard and phase

Additional relevant standards

Validity

Certification Body



Individual FSM number for each certified company

Company Logo

Details of scope of FSM certification

Details of phase activities

Relation to company locations and departments

Listing and publication of FSM certificates

Safety Case Symposium 2018 Singapore

Thank you

Dr. Thorsten Gantevoort
Head of Certification Body, TUV Rheinlan

Safety Case Symposium 2018
Singapore
www.SafetyCaseSymposium.com