Improved safety through smart testing

Congress PROCESS SAFETY – Dordrecht, The Netherlands – 18 May 2022

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

Improved safety through smart testing

1. Introduction
2. IEC 61511 edition 2.0
3. Proof-test challenges versus operation/production uptime
   - IEC61511 - FS standard normative requirements
4. Safety PLC - application program maintenance and testing
   - IEC61511 - FS standard normative requirements
5. Live demonstration
6. Summary

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

1. Introduction

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

About us

- Tino Vande Capelle

- Senior Functional Safety Expert & Trainer, Safety & Security for Industrial Automation and Control Systems SIS & IACS
- FS Senior Expert

  (TÜV Rheinland, # 0109/05, SIS)

- Clemens Van Wiggen

- Technical Consultant Manager at HIMA
- FS Engineer

  (TÜV Rheinland, # 3138/19, SIS)

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

2. IEC 61511 edition 2.0

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

Functional Safety Standards Timeline

1996

IEC 61511
ANSI/ISA 84.00.01 (*)
Functional Safety
SIS for the Process industry sector
(*) modified with additional grandfather clause as per OSHA 29CFR 1910.119

1997

IEC 61508
Safety Lifecycle
quantitative / qualitative approach

ANSI/ISA 84.01
Safety Lifecycle
quantitative approach

2004

IEC 61508
Functional Safety for E/E/PES ed. 2.0
(route 1_H & 2_H, Proven In Use, Systematic Capability SC)

2010

IEC 61511
Functional Safety
SIS for the Process industry sector ed. 2.0
Part 1: 02/16, COR1: 09/16, AMD1: 08/17 (CSV)
Part 2 & 3: 07/16
(route 2_H: Prior Use - no SFF / 2^H Proven In Use, route 1_H SC, SIS Security Risk Assessment)

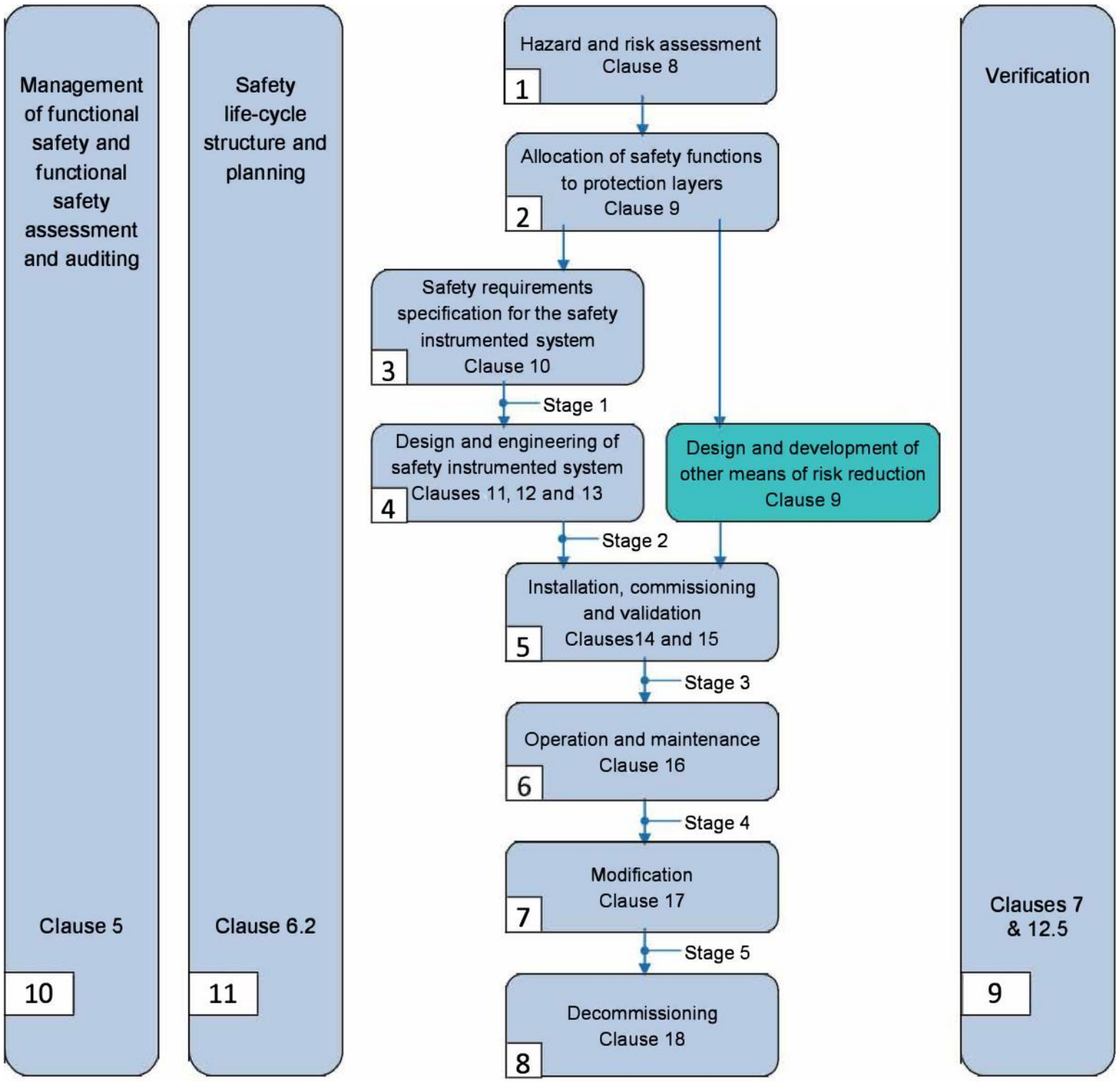
2016 2017

ANSI/ISA 61511
Functional Safety
SIS for the Process industry sector
ISA84 approves IEC61511 ed. 2.0: 09/18

2018

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

IEC61511 SIS safety lifecycle phases



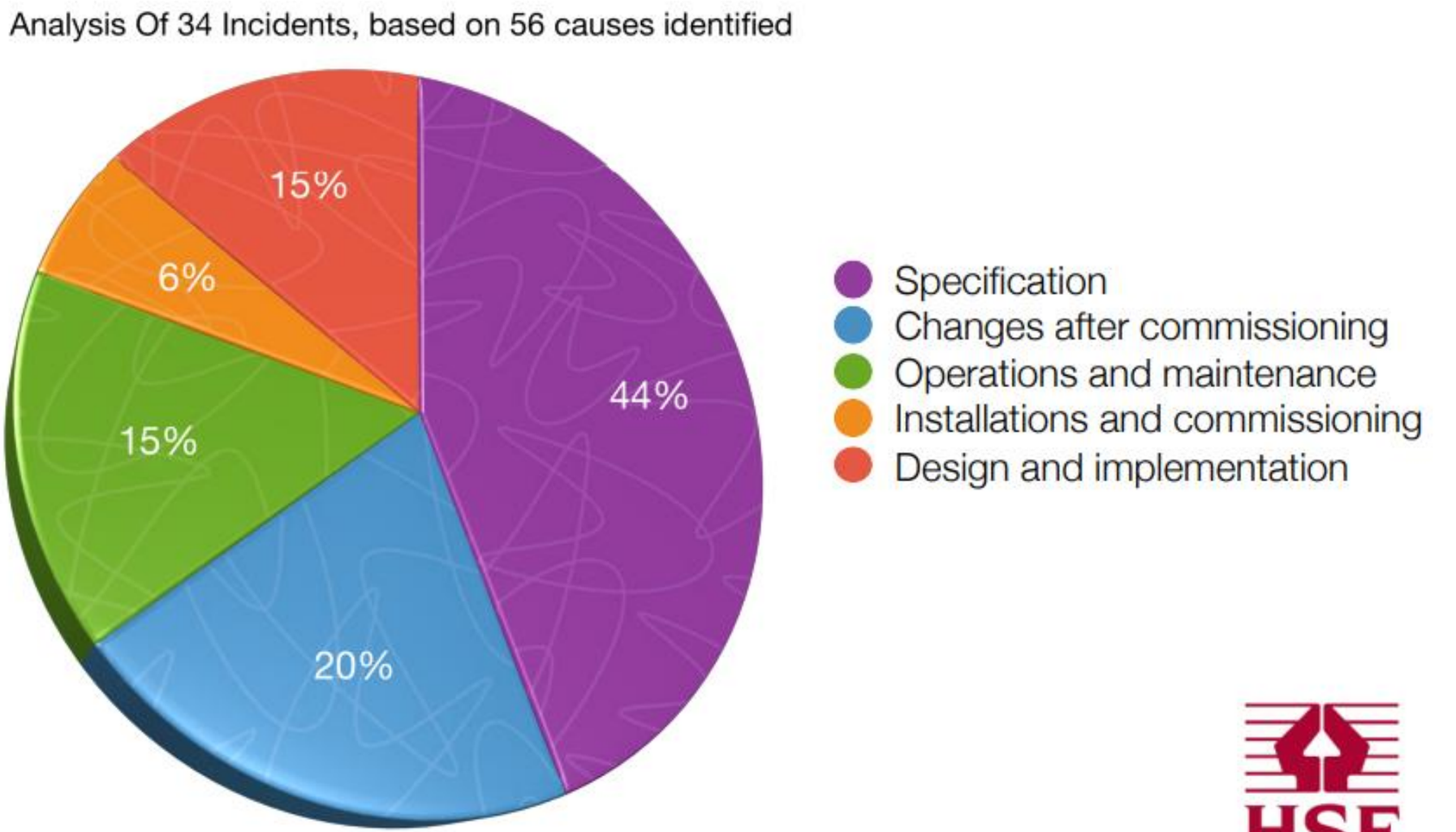
Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

Some of the edition 2.0 key changes

- End USER field QUALITY feedback failure data
- Minimum architecture constraint based on 61511 - Prior Use (route 2H) or - Proven in use (route 2H), alternatively on 61508 – route 1H
- Functional Safety Management for QUALITY life cycle activities
- Functional Safety Assessments – ALL 5 stages EXPERT judgement
- End User / operating company periodic FSA stage 4 – and – FSA stage 5 ‘before’ & ‘after’ any modification
- Safety PLC application programming shall have a 4 eyes principle and evidence how this was achieved

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

3. Proof-test challenges vs production



Out of control: Why control systems go wrong and how to prevent failure?
(2nd edition, source: © Health & Safety Executive HSE – UK)

HSE
Health & Safety Executive

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

Proof-test challenges versus operation / production uptime

- … The never-ending battle between Production & Safety engineers
- Production uptime for management is often (mostly) the priority
- Safety Engineers are often forced to delay the proof test – OR – use unrealistic failures data and proof test intervals to please the production uptime
- And when the proof-test is allowed, it is often during a planned/scheduled shutdown – so what can you proof?
- Additional problem is that the mission time of ANY SIF – subsystem needs to be shorter than the useful lifetime of the same

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

IEC61511 ed 2.0 normative requirements

- The 2nd edition is ALL about QUALITY failure feedback SIF data
- But how do you proof that your safety functions are working without testing under the hazards event conditions?
- "**proof test,** 3.2.56" = *periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition*
- **"Maintenance or testing design requirements,** 11.8" =
  - 11.8.1 The design **SHALL** allow for testing of the SIS either end-to-end or in segments. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line test facilities are required.
  - 11.8.2 When on-line proof testing is required, test facilities **SHALL** be an integral part of the SIS design

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

IEC61511 ed 2.0 normative requirements

- **"SIS operation and maintenance,** 16.2" =
- 16.2.2 Operation and maintenance procedures **SHALL** be developed in accordance with the relevant safety planning and shall provide the following:
  - b) the procedures used to ensure the quality and consistency of proof testing, and to ensure adequate validation is being performed after replacement of any device;

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

4. Application program maintenance/testing

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

Application program maintenance / testing

- Safety PLC programming is no longer called ‘software’ but now ‘application’ programming to distinguish between IEC61511 and 61508 ‘software’ development
- The IEC61511 application programming is defined as Limited Variability Language (LVL) for programmable electronic controllers. The domain to program is vendor related as defined in the safety manual
- But how do you ensure that the programmer or service engineer making a modification doesn’t make a mistake and is understanding the requirement specifications correctly? How can you proof that?

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

a) IEC61511 ed 2.0 normative requirements

- **"SIS application program development,** 12"**,**
  - **"Requirements for application program verification (review and testing),** 12.5" =
  - 12.5.2 The application program including its documentation **SHALL** be reviewed by a competent person not involved in the original development. The approach used for the review and the review results **SHALL** be documented.
  - 12.5.3 The application program, including its decomposition into modules if appropriate, **SHALL** be verified through review, analysis, simulation and testing techniques using written procedures and test specifications, that **SHALL** be carried out to confirm that the application program functions meet the SRS and that unintended functions are not executed and that there are no unintended side effects with respect to the SIF

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

a) IEC61511 ed 2.0 normative requirements

- **"SIS operation and maintenance,** 16**"**,
  - 16.3.1.6 Any change to the application program requires full validation and a proof test of any SIF impacted by the change.
  - 16.3.3 Documentation of proof tests and inspection. The user **SHALL** maintain records that certify that proof tests and inspections were completed as required.

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

5. Live demonstration

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved

Questions?

- In case we run out of time, both speakers can be reached via email on:
  - Tino Vande Capelle: info@tinovc.com
  - Clemens Van Wiggen: c.vanwiggen@hima.com

Copyright © 2004 - 2022 TVC Functional Safety Services FZ-LLC, All rights reserved