Inspecta teollisuusautomaation palvelut
Kumppanisi turvallisuudessa ja luotettavuudessa

IEC 61511 Standardin muutokset

Yleistä

- Epäjohdonmukaisuuksia korjattu
- Kirjoitusvirheitä korjattu
- Päivitetty vastaamaan IEC 61508:2010 ed. 2:sta
- “Should” vaihdettu “shall”:ksi monissa kappaleissa.

IEC 61511 Standardi muutokset

5.2.6. Functional Safety Assessment

FSA-vaatimuksia tarkennettu:

5.2.6.1.4 FSA team shall review the work carried out on all phases of the safety life cycle prior to the stage covered by the assessment that have not been already covered by previous FSAs. If previous FSAs have been carried out then the FSA team shall consider the conclu-sions and recommendations of the previous assessments. The stages in the SIS safety life-cycle at which the FSA activities are to be carried out shall be identified during the safety planning

TRUST & QUALITY www.inspecta.com

IEC 61511 Standardi muutokset

5.2.6. Functional Safety Assessment

FSA myös muutoksille ja käytön aikana:

5.2.6.1.9 In cases where a FSA is carried out on a **modification** the assessment shall consider the impact analysis carried out on the proposed modification and confirm that the modification work performed is in compliance with the requirements of IEC 61511.

5.2.6.1.10 A FSA shall also be carried out periodically during the operations and maintenance phase to ensure that maintenance and operation are being carried out according to the assumptions made during design and that the requirements within IEC 61511 for safety management and verification are being met.

IEC 61511 Standardi muutokset

7.2.2. – 7.2.6 Verification

Todentamisvaatimuksia tarkennettu:

7.2.2 Where the verification includes testing, the **verification** planning shall also address the following:

a) the strategy for integration of **application program** and hardware and field devices,

b) test scope

c) test cases and test data (these will be specific scenarios with the associated data);

d) types of tests to be performed;

TRUST & QUALITY www.inspecta.com

IEC 61511 Standardi muutokset

7.2.2. – 7.2.6 Verification

e) test environment including tools, hardware, all software and required configuration;

f) test criteria (e.g., pass/fail criteria) on which the results of the test will be evaluated;

g) procedures for corrective action on failure during test;

h) physical location(s) (e.g., factory or site);

i) dependence on external functionality;

j) appropriate personnel;

k) management of change;

l) non-conformances.

IEC 61511 Standardi muutokset

7.2.2. – 7.2.6 Verification

7.2.3 Non-safety functions integrated with safety functions shall be **verified** for non-interference with the safety functions.

7.2.4 Verification shall be performed according to the **verification planning.**

7.2.5 During testing, any modification shall be subjected to an impact analysis which shall determine all SIS components impacted and the necessary **re-verification** activities.

7.2.6 The results of the **verification** process shall be available (see 19), including whether the objective and criteria of the tests have been met.

TRUST & QUALITY www.inspecta.com

IEC 61511 Standardi muutokset

8. Process H&RA **(Hazard & risk assessment)**

Tietoturva mukaan vaara- ja riskiarvioon:

8.2.4 A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

a) a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);

b) a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);

c) a description of the potential consequences resulting from the security events and the likelihood of these events occurring;

IEC 61511 Standardi muutokset

8. Process H&RA (Hazard & risk assessment)

d) consideration of various phases such as design, implementation, commissioning, operation, and maintenance;

e) the determination of requirements for additional risk reduction;

f) a description of, or references to information on, the measures taken to reduce or remove the threats.

NOTE 1: Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443:2010.

IEC 61511 Standardi muutokset

9.3 SIL 4 (2003 versiossa)

2003 versiossa SIL4:ää pyrittiin välttämään. Uudessa versiossa helpommin mahdollinen:

9.2.5 In cases where the allocation process results in a risk reduction requirement of >10 000 or average frequency of dangerous failures>10-8 per hour for a single SIS or multiple SISs or SIS in conjunction with a BPCS protection layer**, there shall be a reconsideration of the application** (e.g., process, other protection layers) **to determine if any of the risk parameters can be modified so that the risk reduction requirement of >10 000 or average frequency of dangerous failures>10-8 per hour is avoided.**

IEC 61511 Standardi muutokset

9.3 SIL 4 (2016 versiossa)

9.2.6 If after further consideration of the application and confirmation that a risk reduction requirement >10 000 or average frequency of dangerous failures>10-8 per hour is still required, then consideration should be given to achieving the safety integrity requirement using a number of protection layers (e.g., SIS or BPCS) with lower risk reduction requirements. If the risk reduction is allocated to multiple protection layers then such protection layers shall be **independent** from each other or the lack of **independence** shall be assessed and shown to be sufficiently low compared to the risk reduction requirements.

TRUST & QUALITY www.inspecta.com

IEC 61511 Standardi muutokset

10 SIS safety requirements specification (SRS)

AP vaatimukset lisätty SRS:ään:

10.3.3 The application program safety requirements shall be derived from the SRS and chosen architecture (arrangement and internal structure) of the SIS. The application program safety requirements may be located in the SRS or in a separate document (e.g., application program requirements specification).

10.3.4 The application program safety requirements shall be specified for each programmable SIS device necessary to implement the required SIF consistent with the architecture of the SIS.

IEC 61511 Standardi muutokset

10 SIS safety requirements specification (SRS)

10.3.5 The application program safety requirements specification shall be sufficiently detailed to allow the design and implementation to achieve the required functional safety and to allow a functional safety assessment to be carried out.

IEC 61511 Standardi muutokset

11.4 Hardware fault tolerance (HFT)

Vikasietoisuuteen reitti 2H ja SFF poistettu:

11.4.3 The HFT of the SIS or its SIS subsystems shall be in accordance with;

- 11.4.5 to 11.4.9 of clause 11 or,
- the requirements of 7.4.4.2 (route 1H) of IEC 61508-2:2010 or,
- the requirements of 7.4.4.3 (route 2H) of IEC 61508-2:2010.

(route 1H = IEC 61508 fulfilled, route 2H =proven in use)

IEC 61511 Standardi muutokset

11.4 Hardware fault tolerance (HFT)

Table 5 – Minimum hardware fault tolerance of PE logic solvers

SIL	Minimum hardware fault tolerance		
	SFF < 60 %	SFF 60 % to 90 %	SFF > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

SFF poistettu standardista

TRUST & QUALITY www.inspecta.com

IEC 61511 Standardi muutokset

11.4 Hardware fault tolerance (HFT)

Table 6 – Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers

SIL	Minimum hardware fault tolerance (see 11.4.3 and 11.4.4)
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

IEC 61511 Standardi muutokset

11.4 Hardware fault tolerance (HFT)

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (Any mode)	0
2 (demand mode)	0
2 (continuous mode)	1
3 (Any mode)	1
4 (Any mode)	2

Vikasietoisuusvaatimukset riippuvat toimintatavasta, ei SFF:stä

IEC 61511 Standardi muutokset

11.5.2.1 Devices selected for use as part of a SIS with a specified SIL shall be in accordance with IEC 61508-2:2010 and IEC 61508-3:2010 and/or 11.5.3 through 11.5.6, as appropriate.

Voidaan hyödyntää systemaattista kyvykkyyttä!

IEC 61511 Standardi muutokset

11.5.3 Requirements for the selection of devices based on prior use

Käyttökokemusten perusteella hyväksi todettavien laitteiden vaatimuksia tarkennettu.

IEC 61511 Standardi muutokset

11.9 Quantification of random failure

Vikaantumislaskentaa tarkennettu:

11.9.3 The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified and shall be based on field feedback from similar devices used in a similar operating environment.

11.9.4 The reliability data uncertainties shall be assessed and taken into account when calculating the failure measure.

11.9.5 If, for a particular design, the target failure measure for the relevant SIF is not achieved then:

(4 kohtaa vikaantumisen parantamiseen)

IEC 61511 Standardi muutokset

12 SIS Application Program Development

Sovellusohjelmiston kehittämiseen liittyvä kappale 12 uudelleen muotoiltu.

- Elinkaareen liittyviä vaatimuksia siirretty kappaleeseen 6.
- V-malli poistettu ja siirretty esimerkiksi osaan 2.
- Verifiointivaatimuksia lisätty

IEC 61511 Standardi muutokset

16 SIS operation and maintenance

Turvatoimintojen ohittamiseen varmistusvaatimuksia:

16.2.3 Operation procedures shall be made available. **Compensating measures that ensure continued safety while the SIS is disabled or degraded due to bypass (repair or testing) shall be applied with the associated operation limits (duration, process parameters, etc.).** The operator shall be provided with information on the procedures to be applied before and during bypass and what should be done before the removal of the bypass and the maximum time allowed to be in the bypass state. This information shall be reviewed on a regular basis.

IEC 61511 Standardi muutokset

16 SIS operation and maintenance

16.2.4 Continued process operation with a **SIS device in bypass shall only be permitted** if a hazards analysis has determined that compensating measures are in place and that they provide adequate risk reduction. Operating procedures shall be developed accordingly.

Toiminnallisen turvallisuuden standardit, päivitystilanne

Toiminnallisen turvallisuuden standardit, päivitystilanne

IEC 61508:

- Kansallisten komiteoiden kommentit saatu. Kommentteja käsitellään osien 1/2 ja 3 komiteoiden alatyöryhmissä.
- DIS:n julkaisuaikataulua ei päätetty
- IEC 61508-1/2 kokous oli Irlannissa Limeric:ssä 1.-2.3.2018 (En osallistunut)
- IEC 61508-3 kokous oli Irlannissa Limeric:ssä 27.-28.2.2018
- Seuraavat kokoukset heinäkuun alussa Saksassa

IEC 61508-3 Olio-ohjelmointi turvallisuuteen liittyvissä järjestelmissä (Eli MT61508-3 TS 63177 ED 1, Requirements for object oriented software in safety-related systems) Frankfurtissa 6.-7.3.2018 ja 16.-17.4.2018

IEC TC 65 AHG1 TR Functional Safety & Cybersecurity

IEC 62879/Ed.1 Safety and Human Factors (Viimeisin kokous 2017 joulukuu)

Toiminnallisen turvallisuuden standardit, päivitystilanne

IEC 61511:

- Virallisen työn osuus on päättynyt standardin julkaisemiseen
- Ryhmä tekee ohjeistusta standardin soveltamisesta mm. IEC 61511-0 TR
- Pohtii seuraavan version parannuksia.
- Seuraava kokous Firenze Italia 22.-24.5.2018

TRUST & QUALITY www.inspecta.com