BOŠTJAN NARALOČNIK UNIV. DIPL. INŽ. EL., TUV FSE | PROJECT CTO, COMITA D.D.

POMEN IN VLOGA STANDARDOV

IEC61508 / 511 (FUNCTIONAL SAFETY) PRI MEDNARODNIH PROJEKTIH

1. Uvod

Podjetje Comita d.d. je sistemski integrator, proizvajalec in dobavitelj celovitih tehnoloških rešitev in storitev s področja telekomunikacij, informacijskih tehnologij in industrijske avtomatizacije. Sodelujemo na mednarodnih projektih izgradnje plinovodnih omrežij, naše znanje in tehnologijo pa smo vgradili v več kot 3000 km plinovodov in v več 100 objektov plinovodnih omrežij.

Pridobljene izkušnje in zahteve največjih svetovnih partnerjev od nas terjajo spoštovanje vseh uveljavljenih mednarodnih standardov, zaradi specifične narave tehnološko in varnostno izrazito zahtevnih sistemov pa tudi poseben poudarek na varnosti, k čemur smo zavezani na vseh ravneh našega delovanja. Nadgradnjo obstoječih politik, standardov in procesov predstavlja implementacija ustrezne ravni zagotavljanja funkcijske varnosti.

2. Funkcijska varnost in standarda IEC61508 in IEC61511

Koncept funkcijske varnosti (Functional Safety) v Sloveniji in svetu ni nov ter je že desetletja uveljavljen v prometu, vesoljski in letalski industriji. Zadnja leta pa se je pozornost proizvajalcev in uporabnikov razširila tudi na ostala področja, ki predstavljajo večja tveganja za varnost ljudi, premoženja in okolja. Še posebej to velja za naftno, plinsko in petrokemično industrijo, kjer se najpogosteje srečujemo z zahtevnimi avtomatiziranimi krmilnimi in nadzornimi sistemi. Varnost na objektih in v procesih namreč ne temelji zgolj na ustreznosti vgrajenih naprav ali izpolnjevanju zakonodajnih zahtev, marveč na celovitem (avtomatiziranem) upravljanju, upoštevaje potencialne človeške napake, ki lahko nastajajo pri krmiljenju ali vzdrževanju vgrajenih sistemov.

Funkcijsko varnost posebej obravnavata standarda IEC61508 in IEC61511 (povezava med njima je podana na sliki 1), ki postavljata referenčni okvir za oceno posledic nepravilnega delovanja sistemov in za vzpostavitev kriterijev in dodatnih varovalk za zmanjševanje rizikov nepravilnega delovanja, ki lahko privede do velike ekonomske in okoljske škode ter ogrozi varnost in zdravje zaposlenih. S prepoznanim, ovrednotenim in verificiranim načrtovanjem ter delovanjem varnostnih

sistemov, z možnostjo izračuna potencialnih tveganj in načrtovanjem izboljšav na podlagi beleženja zgodovine ter celotnega projektnega cikla, lahko ob implementaciji standardov dosežemo sprejemljiv/minimalen nivo tveganj oz. ustrezno raven delovanja sistemov, zaradi česar je uporaba navedenih standardov postala praktično obvezna pri vseh projektih izgradnje plinskih omrežij.

> *Standard IEC61508 velja za krovni standard, ki definira osnovne zahteve in zahteve za proizvajalce in dobavitelje tako imenovanih sistemov z varnostnimi instrumenti (Safety Instrumented System – SIS).*

Funkcijska varnost naprave ali sistema (Safety Integrity Level – SIL) je opredeljena na štiristopenjski lestvici od 1 do 4, s tveganostjo procesa pa se viša nivo funkcijske varnosti delovanja varnostnega sistema.

> *Standard IEC61511 obravnava vidike za upravljanje varnosti skozi celoten življenjski cikel sistema (od zasnove, delovanja, vzdrževanja in razgradnje) in je namenjen načrtovalcem in sistemskim integratorjem, ki te sisteme vgrajujejo v proces.*

Opozarja na pomen pravilnega vodenja, planiranja, preverjanja, vrednotenja in revizije procesa načrtovanja varnostnih sistemov.

V nadaljevanju bodo predstavljene bistvene lastnosti standarda IEC61511 oziroma njegova uporaba na podlagi aktualnih izkušenj Comite d.d., pridobljenih ob izvajanju večjega mednarodnega projekta v plinski industriji.

3. Zahteve standarda in življenjski cikel

Da bi se zadostilo zahtevam standarda IEC61511, je potrebno prvenstveno zadostiti zahtevam v poglavjih 5–19:

- Zahteve za vodenje in planiranje funkcijske varnosti (5)
- Življenjski cikel (6)

ZAHTEVE STANDARDA ZA ŽIVLJENJSKI CIKEL

- Preverjanje/verifikacija (7)
- Zahteve življenjskega cikla (8-18)
- Zahteve za dokumentacijo (19)

Posebno pozornost velja na tem mestu posvetiti življenjskemu ciklu. Na sliki 2 je prikazan življenjski cikel sistema z varnostnimi instrumenti (SIS). Kot izhaja iz samega poimenovanja, gre za sistem, ki temelji na instrumentih (merilnikih fizikalnih veličin, aktuatorjih), ki so osnova za varno delovanje procesa.

Življenjski cikel sistema z varnostnimi instrumenti zajema osem faz od načrtovanja do razgradnje, pri čemer velja poudariti, da se določene aktivnosti raztezajo prek celotnega življenjskega cikla procesa (vodenje in planiranje, preverjanje, vrednotenje in revizija):

1. Analiza tveganja
2. Dodelitev varnostnih nivojev k varnostnim funkcijam
3. Izdelava specifikacije za sistem z varnostnimi instrumenti
4. Projektiranje in inženiring

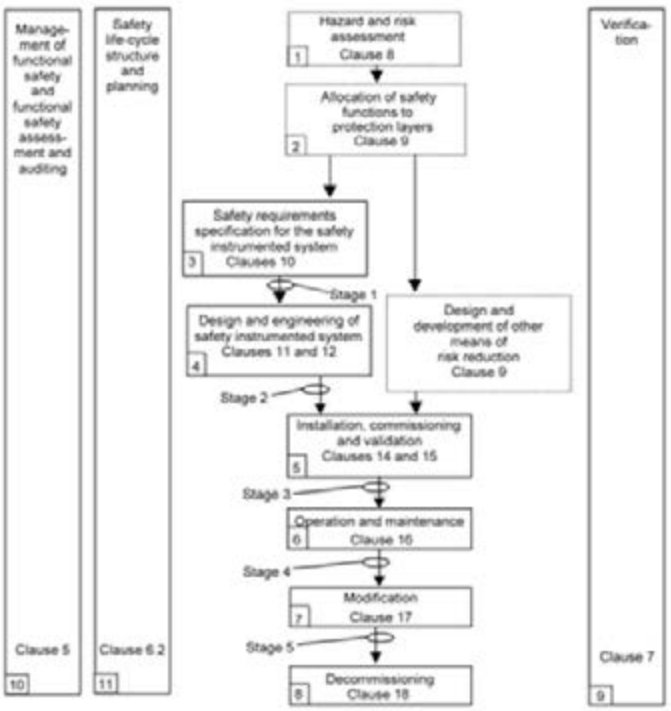

Figure 2 – ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) Safety Life Cycle

NOTE 1 Stages 1 through 5 inclusive are defined in clause 5.2.6.1.3.
NOTE 2 Phases 1 through 11 inclusive are shown. All references are to Part 1 unless otherwise noted.

5. Inštalacija, zagon in validacija
6. Obratovanje in vzdrževanje
7. Modifikacija
8. Razgradnja

4. Vodenje in planiranje

V standardu so za vsako fazo življenjskega cikla podane podrobne tehnične in organizacijske zahteve, zato je vodenje in planiranje postopkov za vse faze življenjskega cikla eden ključnih temeljev vsakega projekta, pri katerem so uporabljeni sistemi z varnostnimi instrumenti.

Osnovni dokument vodenja in planiranja je tako imenovani Functional Safety Management Plan (FSMP), v katerem se podrobneje opredeli:

- **kako podjetje vodi postopke načrtovanja, izvedbe in testiranja sistema z varnostnimi instrumenti, da bo končen produkt skladen z zahtevami standardov (IEC61508-1 / poglavje 6 in IEC61511 / poglavje 5);**
- **vloge in potrebne kompetence oseb za vsako fazo življenjskega cikla;**
- **zagotavljanje neodvisnosti oseb, ki bodo opravljale preverjanje, vrednotenje in revizijo;**
- **plan preverjanja, vrednotenja in revizije;**
- **postopke za spremljanje in obvladovanje sprememb (Management of Change - MOC).**

V standardu so za vsako fazo življenjskega cikla opredeljeni cilji, zahteve, set vhodnih podatkov in dokumentov ter predvideni izhodni rezultati. Velik del zahtev se nanaša na organizacijo in kadre, zato se lahko ti deli integrirajo tudi v splošne politike in akte podjetja. S tem se olajša izdelava načrta za posamezen projekt, saj se pri organizaciji in kadrih lahko sklicujemo na že vzpostavljene interne akte podjetja.

5. Preverjanje (verifikacija)

Standard veleva, da se za vsako fazo oziroma aktivnost procesa opravi neodvisno preverjanje. Preverjanje mora dati odgovor, ali so dosežene zahteve, ki so bile podane za to fazo oziroma aktivnost.

Zato je potrebno za vsako fazo/aktivnost procesa izdelati plan preverjanja, da se natančno ve, kaj je potrebno v tej fazi narediti in kako se narejeno preverja.

Še posebej pomembno je, da se opredeli raven neodvisnosti oseb, ki opravljajo preverjanje. Ta raven neodvisnosti se veča glede na želeno stopnjo SIL. Višja kot je zahtevana stopnja SIL, večja je zahtevana stopnja neodvisnosti oseb, ki opravljajo preverjanje.

6. Vrednotenje in revizija

Vrednotenje in revizija morata dati odgovor na vprašanje, ali je proces načrtovanja in izvedbe projekta voden in izpeljan tako, da je dosežena zahtevana stopnja funkcijske integritete.

Faze vrednotenja in revizije je potrebno načrtovati znotraj FSMP. Predvsem je pomembno, da so člani projektne ekipe, ki opravlja vrednotenje in revizijo, izkušene in kompetentne osebe, ki niso neposredno vpletene v postopke načrtovanja in izvedbe.

> *V veliko pomoč pri načrtovanju so tudi smernice THE 61508 ASSOCIATION, kjer so podana navodila za Oceno skladnosti varnostno povezanih sistemov (Conformity Assessment of Safety-related Systems - CASS).*

7. Dokumentacija

V standardu IEC61511 – poglavje 19, so podane podrobne zahteve za dokumentacijo vezano na „Sistem z varnostnimi instrumenti“. Glavni namen teh zahtev je zagotavljanje, da je za vsako fazo življenjskega cikla na voljo relevantna dokumentacija, ki omogoča:

- **pravilno in učinkovito izvedbo;**
- **preverjanje, vrednotenje in revizijo postopkov in rezultatov.**

Predvsem mora dokumentacijski sistem v podjetju omogočati spremljanje zgodovine sprememb, da se v vsakem trenutku ve, katera je trenutno veljavna in uporabna verzija dokumenta.

8. Primer iz prakse

Comita d.d. kot proizvajalec in sistemski integrator sledi primerom dobre prakse na področju varnosti. Zato smo tudi področje funkcijske varnosti integrirali v politiko kakovosti podjetja, področje funkcijske varnosti pa še dodatno pokrivata

strokovnjaka s TUV certifikatom Functional Safety Engineer oziroma Functional Safety Professional.

Zavedamo se namreč, da za uspešen nastop na trgu in sodelovanje pri večjih projektih ni dovolj le izpolnjevanje zakonodajnih zahtev, splošnih aktov s področja varovanja zdravja, varnosti, okolja, predpisov v specifičnih vejah industrije in temeljnih standardov (npr. ISO9001).

> *Vse pomembneje je, kako obvladujemo procese in kakšni varnostni in okoljski vidiki so pri tem upoštevani. Naprave in procesi morajo biti zanesljivi in varni, zdravje zaposlenih in varovanje okolja pa prioriteta vseh udeležencev projekta.*

Nedavno smo pričeli z izvajanjem večjega mednarodnega projekta s področja plinske industrije, kjer so bile s strani naročnika dane striktne zahteve po upoštevanju določil standardov IEC61508 in IEC61511.

Za zadostitev kriterijem naročnika smo v podjetju sprejeli še dodatne ukrepe in ustrezno politiko funkcijske varnosti.

Kot navedeno v prispevku, smo za projekt najprej izdelali podroben Functional Safety Management Plan, kjer smo opredelili, kako se bo pri izvajanju projekta zadostilo zahtevam iz standardov IEC61508 in IEC61511 in kjer smo natančno opredelili:

- **katere faze življenjskega cikla obsega projekt (v našem primeru so bile to projektiranje in inženiring ter inštalacija, zagon in validacija);**
- **vlogo in kompetence posameznikov, ki bodo opravljali dela povezana s funkcijsko varnostjo;**
- **neodvisnost oseb, ki bodo opravljale preverjanje in vrednotenje rezultatov;**
- **aktivnosti povezane s preverjanjem, vrednotenjem in revizijo;**
- **postopke spremljanja in obvladovanja sprememb za vsako fazo.**

Izdelava FSM plana nam je omogočila boljši pregled nad celotnim izvajanjem projekta, bolje je pripravljena dokumentacija, predvsem pa so vsi sodelujoči na projektu natančno seznanjeni s svojimi nalogami, kar zmanjšuje možnost napak ter projekt časovno in kadrovsko optimizira.

Za zadostitev zahtevam standarda mora tudi naročnik izvajati določene s standardom povezane aktivnosti. Govorimo predvsem o opravljanju revizije, ki je po standardu predvidena po koncu faze projektiranja in po končanem zagonu. Izkazalo se je, da je smiselno revizije opraviti že prej (med samim projektiranjem oz. zagonom), da se lahko tako pravočasno ugotovijo pomanjkljivosti. Tudi na našem projektu je naročnik (oz. s strani naročnika imenovana neodvisna inštitucija) opravil revizijo v dokaj zgodnji fazi izvajanja projekta, zato smo lahko skupaj dopolnili in izboljšali naše postopke.

Projekt se tudi ob upoštevanju zahtev navedenih standardov uspešno nadaljuje in se trenutno nahaja v 4. fazi življenjskega cikla (Načrtovanje in inženiring sistema z varnostnimi instrumenti).

9. Sklep

Pri vseh projektih v procesni industriji, še posebej pa pri projektih izgradnje plinovodnih omrežij, je varnost za ljudi in okolico velikega pomena. To dosegamo z upoštevanjem vseh standardov in s primeri dobre prakse, ki veljajo za ta področja. Za področje funkcijske varnosti sta to standarda IEC61508 in IEC61511.

Naše izkušnje kažejo, da standarda ponujata odličen okvir za zagotavljanje dobre izvedbe projekta, sledljivosti postopkov in dokumentacije. Obenem pa predstavljata dodatno zavarovanje pred odgovornostjo ob morebitnih nepravilnostih.

S tem nadalje ostajamo zavezani celostni varnosti, zdravju zaposlenih ter varovanju okolja, premoženja in opreme.