NESTE ENGINEERING SOLUTIONS

Functional safety assessment

ASAF teemapäivä 19.4.2018

Jari Koivuvirta
Automation, Functional Safety
Neste Engineering Solutions
Mobile: +358 50 458 9756
e-mail: jari.koivuvirta@neste.com
TÜV FSP ID: TP08050126, Safety Instrumented Systems in Process Industry

Customer segments

We Focus on the Process Industry

Biopharma

Food Industry

Biochemicals

Biofuels and Additives

Oil Refining

Petrochemicals

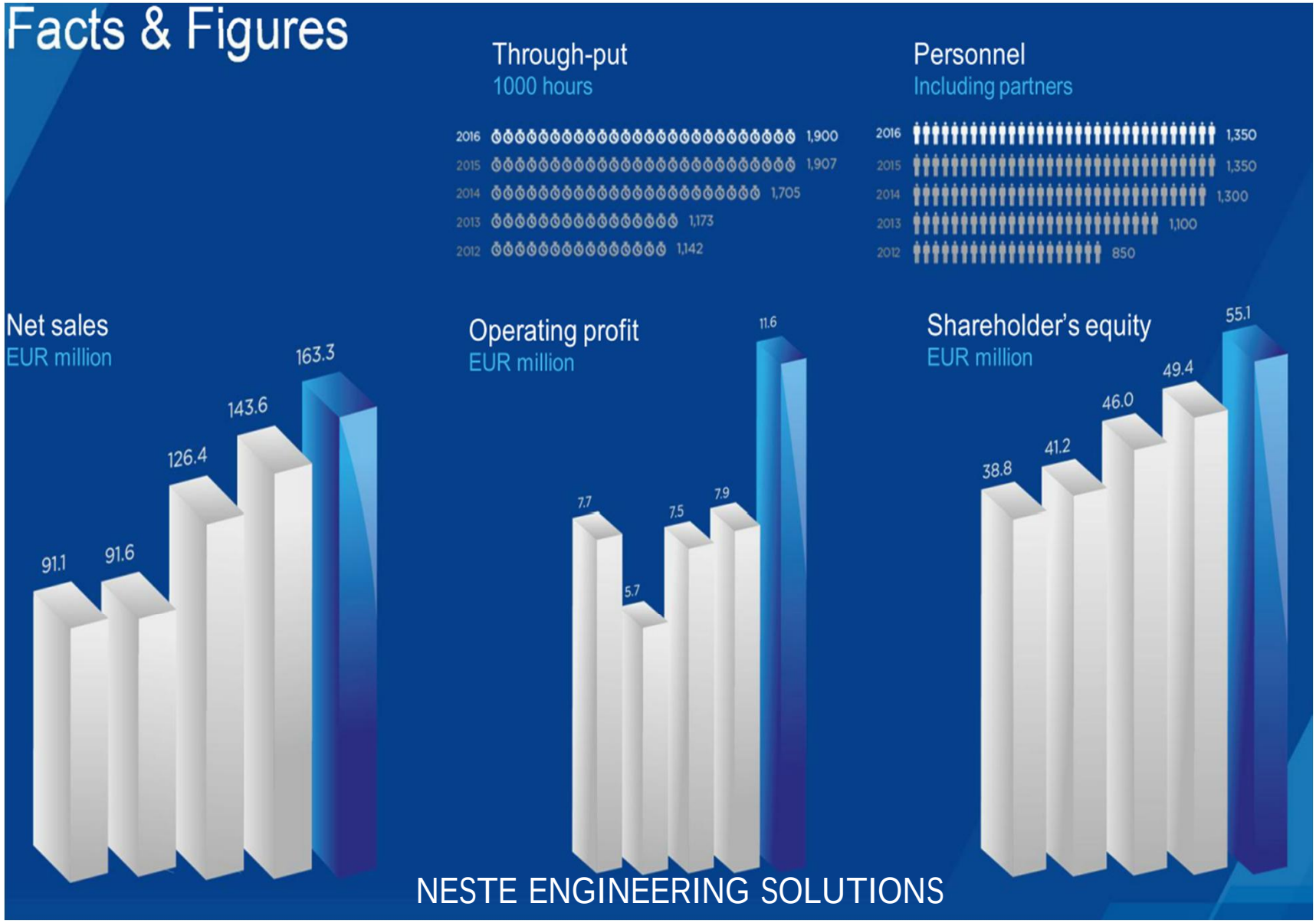
Gas

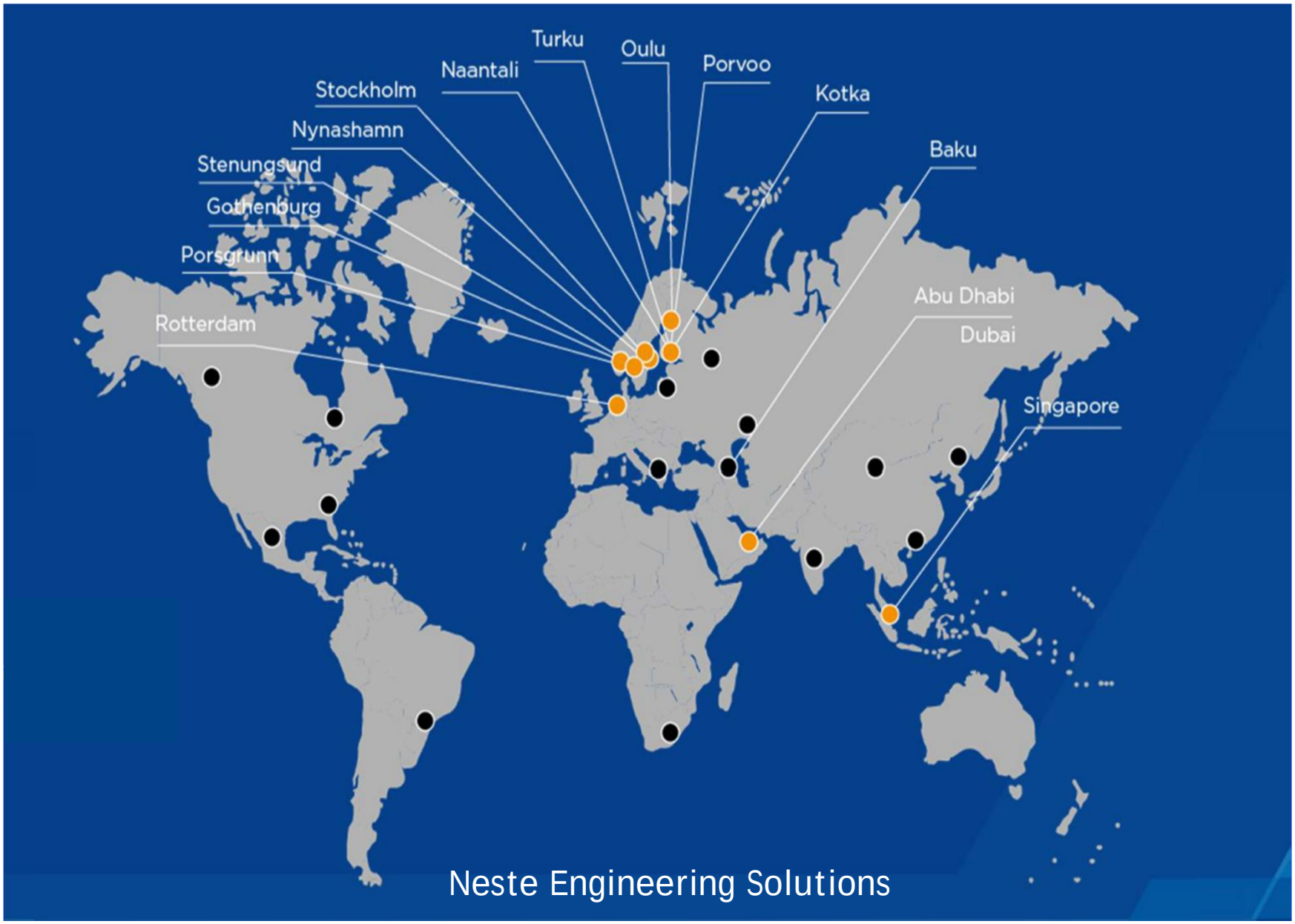
Natural Gas – Biogas - LNG

Utilities

Finish

Neste Engineering Solutions


Facts & Figures
Through-put
1000 hours
2016 1,900
2015 1,907
2014 1,705
2013 1,173
2012 1,142
Personnel
Including partners
2016 1,350
2015 1,350
2014 1,300
2013 1,100
2012 850
Net sales
EUR million
91.1
91.6
126.4
143.6
163.3
Operating profit
EUR million
7.7
5.7
7.5
7.9
11.6
Shareholder's equity
EUR million
38.8
41.2
46.0
49.4
55.1
NESTE ENGINEERING SOLUTIONS


Turku
Oulu
Naantali
Porvoo
Stockholm
Kotka
Nynashamn
Baku
Stenungsund
Gothenburg
Porsgrunn
Abu Dhabi
Rotterdam
Dubai
Singapore
Neste Engineering Solutions

ARVIOINTI, vaiheissa 1 – 7

(virheiden havaitseminen)

Management of functional safety & Functional safety assessment (stages 1-5) and auditing

Clause 5

Safety life-cycle structure and planning

Clause 6.2

1 Hazard & Risk Analysis
Clause 8

2 Allocation of safety functions to protection layers
Clause 9

3 Safety requirements specification for the safety instrumented system
Clause 10

Stage 1

4 Design and Engineering of SIS
Clauses 11, 12 & 13

Design and development of other means of risk reduction
Clause 9

Stage 2

5 Installation, commissioning and validation
Clauses 14 & 15

Stage 3

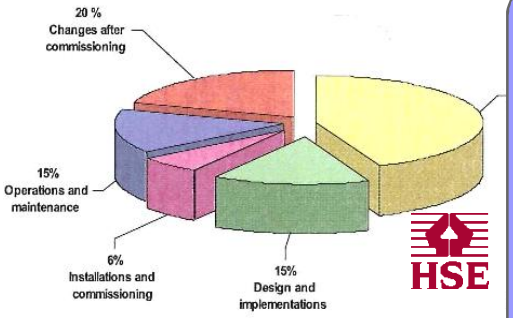
6 Operation & Maintenance
Clause 16

Stage 4

7 Modification
Clause 17

Stage 5

8 Decommissioning
Clause 18



Verification

Clauses 7, 12.5

ARVIOIJAN VALINTA

IEC 61508-1 (logiikkaosan toteutuksen arviointi):

RIIPPUMATTOMUUDEN MINIMITASO	EHEYSTASO			
	1	2	3	4
RIIPPUMATON HENKILÖ	X	X1	Y	Y
RIIPPUMATON OSASTO		X2	X1	Y
RIIPPUMATON ORGANISAATIO			X2	X
Taulukon tulkinta esitetty IEC 61508-1 Ed 2.0 kohdat 8.2.15, 8.2.16 ja 8.2.18				

X = minimi riippumattomuustaso
Y = riippumattomuustaso riittämätön
Valinta X1, X2 riippuu sovelluksen vaativuudesta.
X2 valitaan, jos
• arvioinnin suorittajalla ei ole kokemusta vastaavasta sovelluksesta
• sovellus on vaativa / kohde on uusi / käytettävä teknologia on uutta

Riippumattomuuden lisääntyessä tietämys kohteesta voi vähentyä (?).

ARVIOIJAN VALINTA

IEC 61511-1:
Toiminnallisen turvallisuuden arviointiryhmän jäseniin on kuuluttava vähintään yksi vanhempi pätevä henkilö, joka ei ole ollut mukana projektin suunnitteluryhmässä (vaiheissa 1, 2 ja 3) tai mukana turva-automaatiojärjestelmän käytössä tai ylläpidossa (vaiheissa 4 ja 5).

TOIMINNANHARJOITTAJA VALITSEE ARVIOIJAN
HANKKEEN ALUSSA

- usein ”normaalissa projektissa” toimii yksi asiansa osaava arvioija.

ARVIOINNIN SUUNNITTELU

- Arviointisuunnitelma (lyhyt)
  - Tarkoitus ja tavoitteet
  - Kohde - kohteen erityispiirteet(?)
  - Arviointiperusteet – noudatettu ohjeistus
  - Arvioinnin vaiheistus ja aikataulu

Arvioinnin kaksi näkökulmaa (tukijalkaa)

1. Elinkaarimallin ja laatujärjestelmän (turvallisuussuunnitelma) mukainen toiminta:
   kootaan ”löytyneen” elinkaaridokumentaation statustiedot taulukkoon, joka on arviointiraportin liite **=> parhaimmillaan ”näyttää hyvältä”**

2. Menettelytapojen ja ratkaisujen arviointi:
   Toiminnan seuraaminen livenä, haastattelut ja kysymykset. *Miten tarkastus on suoritettu? Miksi tässä arkkitehtuuri on 2oo2? jne.*
   => parhaimmillaan myös ”tuntuu hyvältä”

ELINKAAREN VAIHEIDEN ARVIOINTI

Koko elinkaari eli kaikki vaiheet arvioidaan ml. johtaminen ja vastuiden määrittely sekä turvatoimintojen riippumattomuus; tarkemmin tutkitaan:

Vaara- ja riskianalyysi (esim. Hazop)

- Osallistujat, kirjausten laatu, tarkempaan SIL-analyysiin määräytyminen

Turvallisuusvaateiden kohdentaminen / vaatimusmäärittely (SIF, SIL)

- Arviointi, mielellään ennen massiivista turva-automaatiosuunnittelua

Tehdastestaus (FAT), toiminnan seuranta

- Koestukset, muutosten hallinta, haastattelut
- Tietoturvan koestus

SAT ja 1. Määräaikaiskoestus, toiminnan seuranta

Arviointi >< Tarkastus

ARVIOINTI, aloitus mahdollisimman aikaisin

(virheiden havaitseminen)

Management of functional safety & Functional safety assessment (stages 1-5) and auditing

Clause 5

Safety life-cycle structure and planing

Clause 6.2

1 Hazard & Risk Analysis
Clause 8

2 Allocation of safety functions to protection layers
Clause 9

3 Safety requirements specification for the safety instrumented system
Clause 10

Stage 1

4 Design and Engineering of SIS
Clauses 11, 12 & 13

Design and development of other means of risk reduction
Clause 9

Stage 2

5 Installation, commissioning and validation
Clauses 14 & 15

Stage 3

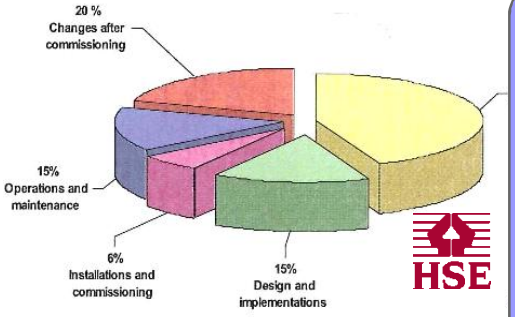
6 Operation & Maintenance
Clause 16

Stage 4

7 Modification
Clause 17

Stage 5

8 Decommissioning
Clause 18



Verification

Clauses 7, 12.5

ELINKAAREN VAIHEIDEN ARVIOINTI

Käynninaikainen arviointi (seisokin yhteydessä)

- Määräaikaiskoestukset
- Käyntijakson aikana tapahtuneet suojaukset
- Kunnossapidon tekemät muutokset
- Suojausten ennakkohälytysten ja muiden ”läheltäpiti” tilanteiden käsittely
- Toimintaohjeet ja koulutus – operaattori osana turvatoimintoa
- Tietoturvallinen toiminta, Varmuuskopiointi. Tietoturvan ylläpito

ARVIOINNIN, RAPORTOINTI (raportista julkaistaan 1-3 revisiota)

Havainnot:
- eivät edellytä toimenpiteitä.

Suositukset:
- jäävät projektiorganisaation / laitoksen haltijan harkintaan; huomioitavaksi toiminnan kehittämisessä.

Huomautukset:
- edellyttävät lisäselvityksiä tai täydentäviä toimenpiteitä.

Poikkeamat: vaativat korjaavia toimenpiteitä;
poikkeamat pitää antaa välittömästi tiedoksi poikkeamista vastaaville suunnittelijoille sekä laitoksen haltijalle.

Havainto (esimerkki):
Automaatiosuunnittelu on (turvallisuussuunnitelman mukaisesti) järjestänyt suunnittelukatselmointeja, joissa on katselmoitu olennaista suunnitteluaineistoa. Suunnittelukatselmoinneissa on olut läsnä asiakkaan edustus, suunnittelun tehnyt suunnittelija sekä automaation pääsuunnittelija ja/tai turvallisuusinsinööri.

ARVIOINTI, RAPORTTI

Poikkeama (esimerkki):
Hyväksyntää SIL-määrittelyssä sekä -todentamislaskennassa tehdyille suunnitteluspesifikaatioiden poikkeamisille ei voitu arviointihetkellä todeta. Ko. seikkoja ovat ratkaisut joihinkin taloudellisiin riskeihin varautumisessa sekä mahdollisesti riskiä pienentävät hyvin nopeat operaattorin toimintavasteet, jos niitä on määritelty (ks. huomautus 2).

Arvioijalle on toimitettava käytönvalvojan tai laitoksen kokonaisturvallisuudesta vastaavan muun tahon allekirjoittama asiakirja/asiakirjat suunnitteluohjeista poikkeamisien hyväksymisestä.

ARVIOINTI, RAPORTTI

Huomautus (esimerkki):
FAT-vaihe. Muutosten lokitaulukon kirjaamiskäytäntö ei täysin vastaa ohjeistusta (turvallisuus-suunnitelman kohta 5 ja ohjeen ...)

Muutosloki on päivitettävä ohjeistuksen mukaisesti; samalla voidaan vielä varmistaa muutosten asianmukainen luokittelu (vähäinen / merkittävä) ja käsittely.

VAARAN PAIKKOJA

Hazop

Muutokset **projektin aikana**

Suunnittelu

Tiedon siirtyminen elinkaaren vaiheiden välillä, puutteellinen tarkastus

Vaikeneminen

Turha byrokratia