Verificatie van de applicatiesoftware is vaak lastig, maar dynamische simulatie is zinvol

Simulatie van PLC applicatie soft

Een dynamische simulatie aan het eind van de engineering fase verhoogt de kwaliteit van de procesveiligheid, maar bovendien zijn er voordelen van zo'n dynamische simulatie ten opzichte van de meer conventionele Factory Acceptance Test.

Herman Jansen
TÜV Certified Functional Safety Expert

Opbouw instrumentele beveiligingen

Omstreeks 2000 is 'SIL' geïntroduceerd als onderdeel van 'functionele veiligheid'. Instrumentele beveiligingen bestaan uit sensoren, een 'logic solver' (meestal een veiligheid PLC) en 'final elements' (meestal kleppen en motoren). De sensoren, final elements en logic solver zijn (of worden) zichtbaar. Merk, types en eigenschappen zijn bekend. Faalgegevens zijn meestal beschikbaar. De bekabeling/bedrading kan gecontroleerd worden.
De programmeerbare functies in de PLC zijn ook een heel wezenlijk onderdeel de 'functionele veiligheid'. Echter de controle van de applicatiesoftware (IEC 61511 2e editie noem dit 'application program') is niet altijd makkelijk uit te voeren.

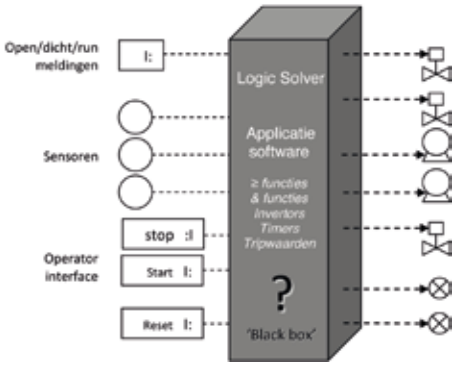


Fig. 1 Schematische weergave van instrumentele beveiligingen

Verloop SIL project

Een gebruikelijk SIL traject is in fig. 2 weergegeven. Gevaren worden geïdentificeerd (bijvoorbeeld door een HAZOP studie) en risico's worden bepaald (SIL classificatie of LOPA). Instrumentele beveiligingen (IEC 61511 noemt die 'Safety Instrumented Functions', afgekort: 'SIFs') worden ontworpen en de gedetailleerde 'functional safety' functies worden uitgewerkt door een slimme designer. Veel later in het project worden dan de geprogrammeerde functies gecontroleerd; soms 'in het veld' en soms bij de PLC leverancier.

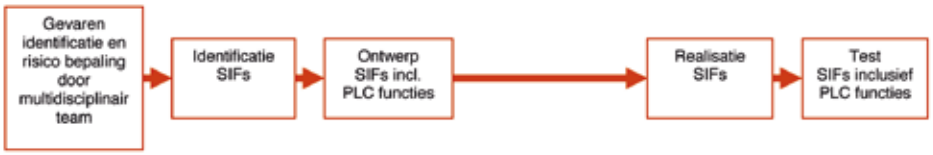


Fig. 2 Gebruikelijk verloop SIL-project

Het kan echter zinvol zijn om tussen ontwerp en realisatie een verificatie van de ontworpen applicatie software uit te voeren. Met name in de volgende situaties:
- Complexe logische functies (bijvoorbeeld in geval van een sequentiële besturing zoals voor een brander installatie).
- Om in een constructie van 'Eindgebruiker - Contractor' te kunnen confirmeren dat het ontwerp van de functionele veiligheid correspondeert met de initiële gevarenidentificatie, risicobepaling en projectdefinitie. De Contractor kan verantwoording afleggen en de eindgebruiker ziet wat hij krijgt en kan zonodig bijsturen zonder grote financiële of planning technische gevolgen.
- IEC 61511 geeft nog aanvullend aan: 'Personnel that will be operating the process should attend since it will give them some early training on the operation of their SIS. Often, they can also provide good suggestions or enhancements to the test procedures that were not foreseen during the design'.

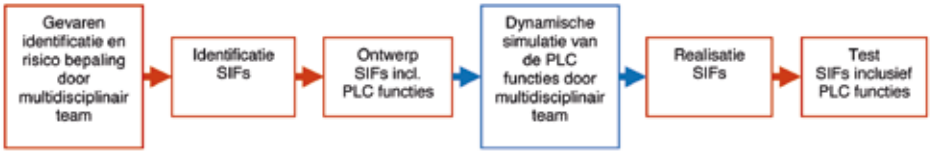
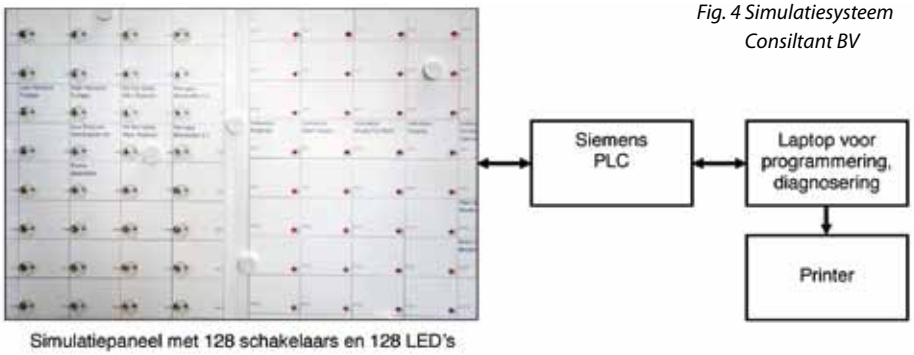


Fig. 3 SIL traject met dynamische simulatie

Het simulatiesysteem



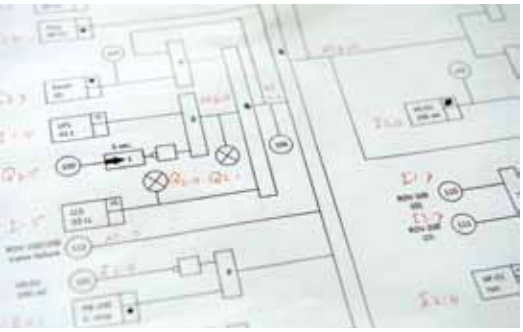
Simulatiepaneel met 128 schakelaars en 128 LED's

Fig. 4 Simulatiesysteem Consiltant BV

Het simulatiesysteem van Consiltant BV bestaat uit een PLC systeem en een simulatiepaneel. De tagnummers/omschrijvingen van de betreffende in- en uitgangen worden op het bord aangegeven.

De 3-standen schakelaars kunnen met een simpele handweging op een logisch '1' of '0' gezet worden. In de derde stand kan de betreffende ingang automatisch worden aangestuurd. Op deze wijze kunnen sensoren automatisch worden aangestuurd. Hierbij kan gedacht worden aan eindschakelaars van kleppen, runcontacten van motorsturingen, lage druk/flow sensoren in de pers van een pomp/ventilator, vlamdetectie, etc. De simulatie wordt hierdoor dynamisch.

ware tijdens de engineering fase



Functional Logic Diagrams

Detail simulatiepaneel

Gebruik van het simulatie systeem

Al voor het SIL tijdperk werd door gerenommeerde internationale olie- en gasbedrijven gebruik gemaakt van simulatie van de ontworpen applicatiesoftware. Men wilde zekerheid dat de door een ingenieursbedrijf ontworpen logische functionaliteit helemaal goed was. Niet alleen de 'Shut Down' maar ook de 'Start-up'. Er werd getest op basis van Cause & Effect diagrammen en de start-up procedure.

Nu in het SIL tijdperk is het belang om zeker te stellen dat beveiligingen zullen functioneren, alleen maar sterker geworden en geformaliseerd in de SIL norm IEC 61511 (2e edition):

- The application program shall be reviewed by a competent person not involved in the original development.
- Application program testing may take place initially on a simulator. The purpose of the initial testing phases (simulation and testing against the design specifications) is:
- 1) to demonstrate that the application program modules provided the necessary functionality and are incapable of any prohibited behaviour;
- 2) to subject the application program to a wide range of conditions and sequences to show that it is resilient to unexpected behaviour.

De operator simuleert hoge druk

Een test team aan het werk

De engineer controleert

Samenvatting

Dynamische simulatie aan het eind van de engineering fase verhoogt de kwaliteit.

De voordelen van simulatie 'in een comfortabele besprekingskamer' t.o.v. de 'Factory Acceptance Test' zijn als volgt:

- Het ontwerp wordt op een overzichtelijke wijze zichtbaar.
- Door de dynamische simulatie kan het ontwerp grondig getest worden.
- Consensus tussen Opdrachtgever en Contractor met betrekking tot de functionaliteit.

Latere afnametesten blijven nodig maar zijn veel minder tijdrovend.

Voor meer informatie:
www.consiltant.com