Nieuwe standaard schept nieuwe mogelijkheden

Veiligheid is programmeerbaar

Met de standaard IEC61508 voor functionele veiligheid is de weg vrijgemaakt voor implementaties in netwerken. De eerste toepassingen zijn voor DeviceNet, maar EtherNet/IP en vervolgens ControlNet gaan dezelfde specificatie realiseren. Rockwell Automation integreert veiligheid in haar Integrated Architectures, en specifiek in haar RSLogix 5000 programmeersoftware en de NetLinx netwerkstrategie.

HANS VAN THIEL

Veiligheid wordt in industriële toepassingen van oudsher onafhankelijk uitgevoerd van de productiesystemen. Daar zijn goede redenen voor. In de eerste plaats moeten veiligheidsfuncties natuurlijk gegarandeerd zijn, juist in het geval van storingen in machines of hun besturingen. Standaarden voor veiligheid waren er dan ook op gericht om die onafhankelijkheid af te dwingen door middel van strenge voorschriften. In de tweede plaats was die losstaande uitvoering van veiligheid dus een vereiste om aan specifieke regelgeving te kunnen voldoen. Een onbedoeld gevolg was echter dat control-systemen voor veiligheid niet goed konden meegroeien met de technologische ontwikkelingen in de industriële automatisering. Veiligheidstechnologie raakte verouderd.
De ontkoppeling van veiligheid en control werkte bovendien in de hand dat veiligheid niet werd geïntegreerd in het ontwerp van industriële besturingen, maar als een systeem daarop en daarnaast werd ontwikkeld. Dat verhoogt echter de complexiteit van het geheel en vergroot de kans op fouten.

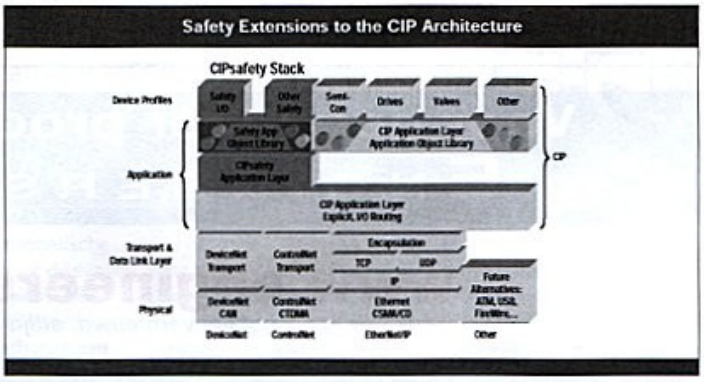
IEC 61508

De recente veiligheidsstandaard 61508 van de IEC (International Electrotechnical Commission) schept echter nieuwe mogelijkheden. IEC61508 bestrijkt alle systemen waarin een of meer elektrische, elektronische of programmeerbare elektronische 'devices' zijn toegepast. De norm is niet van toepassing op gevaren van de apparaten zelf, bijvoorbeeld elektrische schokken, maar op de gevaren ten gevolge van het falen van veiligheidsfuncties. De uit zeven delen bestaande standaard is uitdrukkelijk bedoeld voor veiligheidssystemen in hun totaliteit en omvat niet alleen sensoren en actuatoren maar ook de menselijke operators. Als voorbeelden worden genoemd: noodstopsystemen, spoorwegsignaleringssystemen, dynamische positionering, turbine control en nog andere.

IEC61508 is in 2001 geratificeerd door het Europese comité voor Elektrotechnische Standaardisatie CENELEC en vervangt bij eventuele conflicten alle voorgaande CENELEC- en CEN- (Europees Comité voor Standaardisatie) normen.
Een veiligheidsgerelateerd systeem kan, volgens IEC61508, op zichzelf staande apparatuur zijn, bijvoorbeeld een brandmelder, maar ook deel uitmaken van een ander systeem, bijvoorbeeld de motorsnelheid in een draaimachine. Kenmerkend van deze standaard is dat hij, in tegenstelling tot eerdere normeringen, zich niet meer richt op de uitvoering maar op het resultaat van veiligheidsfunctionaliteit. Zo is de classificatie in een van de vier SIL- niveaus (Safety Integrity Level) niet gekoppeld aan een (sub)systeem of een component, maar aan de veiligheidsfuncties die dat (sub)systeem of die component implementeert.

CIP

Hiermee is de weg vrijgemaakt voor de uitvoering van veiligheidsfunctionaliteit in verschillende technologieën. De ODVA (Open DeviceNet Vendors Asso-



Veiligheidsfunctionaliteit wordt gerealiseerd in CIP (Common Industrial Protocol) dat onafhankelijk is van onderliggende netwerken (Bron: 'Safety Networks', white paper van ODVA (Open DeviceNet Vendor Association).

ciation) heeft dan ook een specificatie uitgebracht, CIPsafety, voor gebruik in het Common Industrial Protocol (voorheen Control and Information Protocol genoemd). CIP is een suite netwerkservices die speciaal ontworpen zijn voor industriële automatisering, bovenop de fysische-, datalink- en netwerklagen. Die onderste lagen kunnen met verschillende technologieën worden gerealiseerd en op dit moment zijn dat DeviceNet, ControlNet en EtherNet/IP.

DeviceNet is een implementatie van de CAN protocollagen en ControlNet is in wezen een uitbreiding daarvan op een nieuwe fysische laag. Het heeft een hogere snelheid, determinisme, herhaalbaarheid en redundantie en is bedoeld voor grotere afstanden. De 'IP' in 'Ethernet/IP' staat voor 'Industrial Protocol' en niet voor 'Internet Protocol' hetgeen enigszins verwarrend is omdat, in de praktijk, tussen Ethernet en CIP nog de Internet protocollen IP en TCP of UDP worden gebruikt.

Ethernet/IP beschrijft dan de inkapseling van CIP in Internet Protocol frames en een groot voordeel is dat de hele Internettechnologie beschikbaar komt. Een voorbeeld is HMI door middel van een standaard webbrowser.

Een netwerkknoop in CIP is een verzameling objecten en een object is een abstracte representatie van een component in een product. CIP is dus objectgeoriënteerd, waarbij een individuele component een instantiëring is van een klasse soortgelijke componenten. Klassen en instantiëringen hebben attributen en leveren diensten die allemaal een unieke identificator bezitten. Het CIP protocol is connectie gebaseerd en elke connectie krijgt ook weer een eigen ID, die echter afhankelijk is van het onderliggende netwerk. Voor DeviceNet is die gebaseerd op het CAN Identifier Field.

Het Common Industrial Protocol en de genoemde netwerken zijn gespecificeerd door de ODVA (Open DeviceNet Vendor Association), CI (ControlNet International) en de IAONA (Industrial Automation Open Networking Alliance), en implementaties van fabrikanten moeten moeiteloos met elkaar kunnen samenwerken. Hetzelfde geldt voor CIPsafety dat begin 2005 is toegevoegd aan de CIP Networks Library. Veiligheid kan nu evenals control-, synchronisatie-, motion-informatie en -configuratie worden geïntegreerd over meervoudige netwerken. Voorlopig geldt dat weliswaar alleen nog voor DeviceNet, maar de specificatie voor Ethernet/IP is gepland voor 2006 en daarna volgt die voor ControlNet.

GuardLogix

ODVA heeft meer dan driehonderd leden waaronder ABB, Siemens, AMCI, Applied Robotics en Cisco. Ook Rockwell Automation is, als oorspronkelijk ontwikkelaar van DeviceNet, een vooraanstaand lid en heeft zich gecommitteerd aan CIP en de ondersteunende netwerken.

De veiligheidsfunctionaliteit in CIPsafety past verder naadloos in het RA Integrated Architecture concept van hardware- en softwareintegratie voor industriële automatisering.

De veiligheidsmodule GuardLogix van Rockwell Automation is dan ook een van de eerste producten die DeviceNetsafety implementeert. De software programmeeromgeving hiervoor is de RSLogix 5000 ontwikkelomgeving die ook voor alle andere oplossingen van dit bedrijf wordt gebruikt. Veiligheidsfuncties zijn hierin strikt gescheiden van de bedrijfsfuncties, zodat veiligheid op geen enkele wijze daarvan afhankelijk kan zijn.

In de hardware wordt veiligheid geïmplementeerd door een dubbelslots CPU, waarmee de Safety-taak extra wordt gecontroleerd. In dit 'CPU-paar' kunnen ook de standaard control-, motion- of procestaken meedraaien. Als wapen tegen netwerkstoringen worden veiligheidsframes in het netwerk dubbel verstuurd en krijgen ze een 'timestamp'. Uiteraard zorgt de veiligheidsfunctie er voor dat, als een storing wordt gedetecteerd, het systeem overgaat naar een veilige toestand. Zo wordt dus de onafhankelijkheid van veiligheidsfuncties gerealiseerd door een logische scheiding in plaats van door een fysieke scheiding, zoals vroeger. Dit bespaart niet alleen op de kosten, met name van bekabeling, maar vergroot ook de mogelijkheden. Veiligheidsrisico's en de te treffen maatregelen kunnen flexibeler en nauwkeuriger worden bepaald en sneller worden geïmplementeerd. Bij een storing in een robot aan het eind van een productielijn, bijvoorbeeld, hoeft misschien niet de hele keten te worden stilgelegd, maar kan een veilige toestand worden bereikt door alleen die productiecel te sluiten.

Toevoeging van diagnostiek en integratie in veiligheidsfuncties is nog een interessante mogelijkheid van CIPsafety. Diagnostiek van de controller, het netwerk, I/O-devices, firmware en respons op applicatieniveau komen allemaal langs dezelfde weg beschikbaar en kunnen dus gemakkelijker worden geïntegreerd.

Het gebruik van dezelfde ontwikkelomgeving, zoals bijvoorbeeld RSLogix 5000, voor bedrijfsbesturing en veiligheidsfuncties, heeft nog een groot voordeel. Veiligheidssystemen worden niet meer bovenop en naast de besturingssystemen ontworpen, maar als samenhangend gedeelte van een algehele oplossing. Dat vermindert de complexiteit en verkleint de kans op ontwerpfouten. ■