GEVAAR ONVERWACHTE RESET OF HERSTART NIET (H)ERKEND

RESETFUNCTIE ALS VEILIGHEIDSFUNCTIE NADER BESCHOUWD

Stel, je moet onderhoud verrichten aan een 120-tons pers. Je loopt de met lichtschermen beveiligde ruimte in en gaat aan de slag. En dan valt er plotseling een bitje om in de PLC en de resetfunctie wordt geactiveerd. Je leven hangt op dat moment af van één enkele startknop! Je zou denken dat dit niet mogelijk is, maar de realiteit is anders…

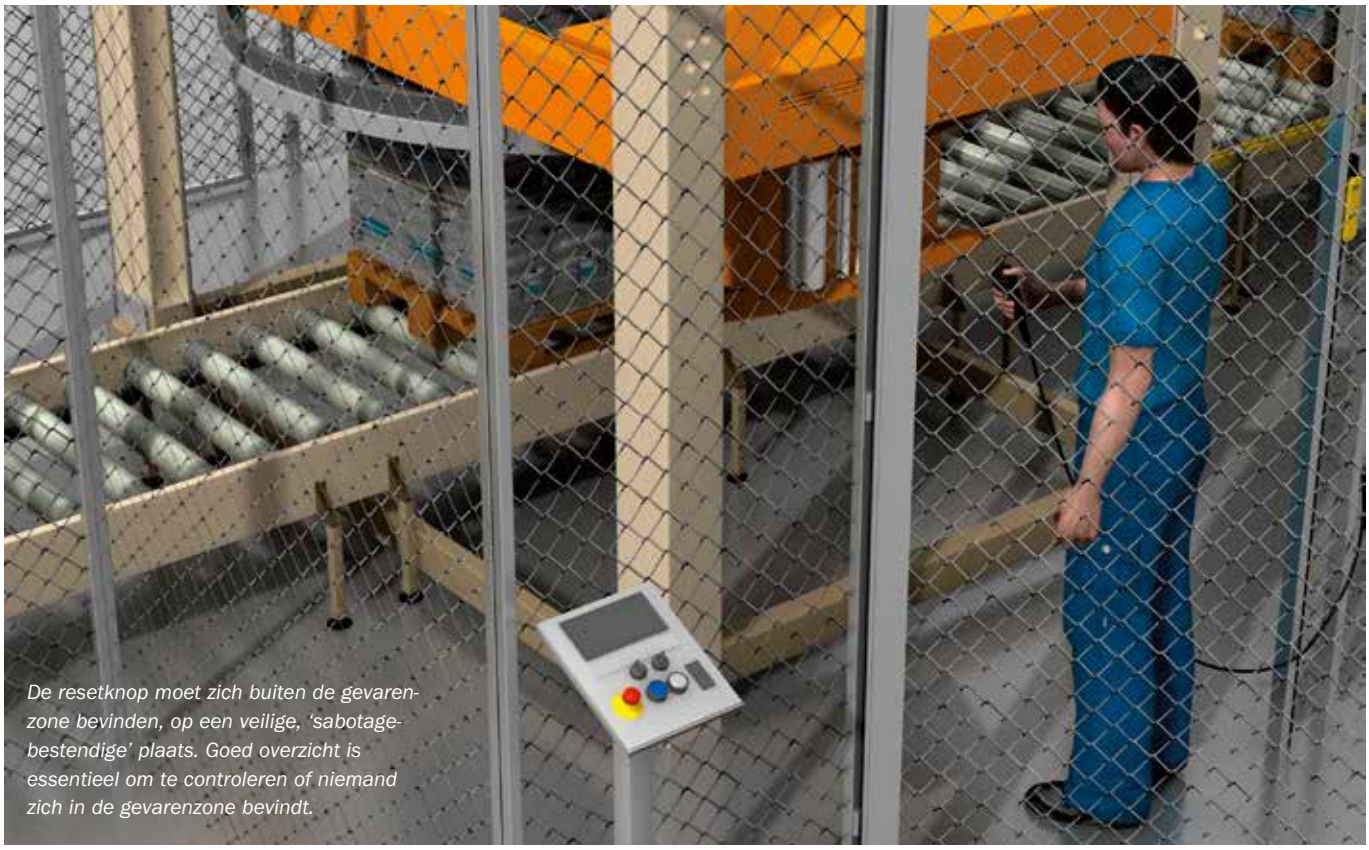
Bedrijven investeren veel in veiligheids-lichtschermen en de daarmee verbonden beveiligingen, maar het voorkomen van onverwachts opstarten zou gewoon via de standaardbesturing moeten en mogen worden geregeld. Dit is een reëel gevaar dat door velen over het hoofd wordt gezien. Er is te weinig aandacht voor en SICK probeert hierin verandering te brengen.

EISEN VOOR EEN RESET

'Reset' is de handbediende functie die alle veiligheidsfuncties (zoals noodstopknop, functieblokkering op toegangsdeuren en lichtschermen) terugstelt, voordat een (her)start mogelijk is. Er worden de nodige eisen aan de reset gesteld:

- Een reset moet worden gerealiseerd door een aparte handbediende actie.
- Een reset moet garanderen dat alle beveiligingen operationeel zijn. Zonder deze garantie mag resetten niet mogelijk zijn.
- Een reset mag geen beweging starten en mag geen gevaarlijke situatie veroorzaken.
- Een reset moet de besturing voorbereiden op een daaropvolgend startsignaal.
- De resetknop moet zich buiten de gevarenzone bevinden op een veilige, 'sabotagebestendige' plaats van waaruit personen een goed overzicht hebben op de gevarenzone. Zo kunnen zij controleren dat zich geen andere personen binnen de zone bevinden.

SICK
Sensor Intelligence.



De resetknop moet zich buiten de gevarenzone bevinden, op een veilige, 'sabotagebestendige' plaats. Goed overzicht is essentieel om te controleren of niemand zich in de gevarenzone bevindt.

GEVAAR OP DE LOER

Tot zover de theorie. De praktijk is nogal eens anders en weerbarstiger. Door externe invloeden op het besturingssysteem of bij storingen in het systeem kan er zomaar een onverwachte reset optreden. Ook kan dit gebeuren als na het wegvallen van de netspanning deze weer wordt ingeschakeld. Kortom, er hoeft maar een bitje om te vallen en je krijgt een soort kettingreactie die funest kan zijn voor de monteur die toevallig onderhoud pleegt aan de pers.

Het gevaar van een onverwachte reset of herstart wordt nog steeds over het hoofd gezien. Daarom meent SICK dat de resetfunctie als veiligheidsfunctie nader moet worden beschouwd. Zeker als iemand zich tussen de beschermende maatregel en het gevaar kan begeven, zonder gedetecteerd te worden.

VEILIGHEIDSFUNCTIES

Waar gaat het precies om bij een veiligheidsfunctie? In de norm EN-12100 wordt een definitie gegeven: een fout in de veiligheidsfunctie resulteert in een onmiddellijke verhoging van het risico. Volgens EN-13849-1: een veiligheidsfunctie wordt uitgevoerd door een veiligheidssysteem om een veilige situatie van een machine en/of systeem te bereiken of te behouden.

Het ontwerp of de uitvoering van een veiligheidsfunctie is maatgevend voor de kwaliteit van de benodigde risicoreductie. Verder wordt de veiligheidsfunctie bepaald in de gevaren- en risicoanalyse en moet deze minimaal de volgende basisitems bevatten:

detectie

logica

beweging

tijdslimieten (indien nodig)

Dit wordt in de norm weergegeven als 'subsystemen'. Bij veiligheidsfuncties gaat het bijvoorbeeld om het permanent of tijdelijk verhinderen van toegang (bijvoorbeeld met als subsysteem lichtschermen of veiligheidsdeuren), het initiëren van een machinestop, het voorkomen van onverwachts opstarten, het verhinderen van opstarten, en muting (het onderscheid maken tussen mens en materiaal). De subsystemen, bijvoorbeeld veiligheidslichtschermen of veiligheidscontrollers, worden vastgesteld voor de berekening en evaluatie van een veiligheidsfunctie. Voor deze subsystemen worden Performance Level (PL) volgens EN 13849-1, dan wel Safety Integrity Level (SILcl) volgens EN 62061, bepaald.

VLIEG OP HET TOUCHSCREEN

De praktijk is dat we veel geld uitgeven aan inloopbeveiligingen in de vorm van lichtschermen en veiligheidsdeuren om te voorkomen dat iemand bij een draaiende machine of robot in de buurt kan komen. Die beveiligingen moeten ook nog eens goed geïntegreerd worden in de veiligheidsbesturing en dat moet allemaal getest worden. Maar als een onderhoudsmonteur naar binnengaat om iets te doen aan de machine, is hij opeens afhankelijk van een resetsignaal!

En hoe wordt dat signaal afgegeven? Door een druk op een knop of een touchscreen. En hoe wordt dat signaal afgevraagd? Via een standaardbesturing. Die monteur is zich van geen gevaar meer bewust, want die denkt dat hij door het veiligheidssysteem beveiligd is. Maar uiteindelijk is het de zwakste schakel die het veiligheidsniveau bepaalt. Er zijn op YouTube-filmpjes te vinden van een vlieg die op een touchscreen landt en zo een Windows-programma opstart. Op een HMI zou dit een reset hebben kunnen veroorzaakt. Daarnaast wordt een HMI ook nog eens door een standaardbesturing afgevraagd.

OPWAARDEREN

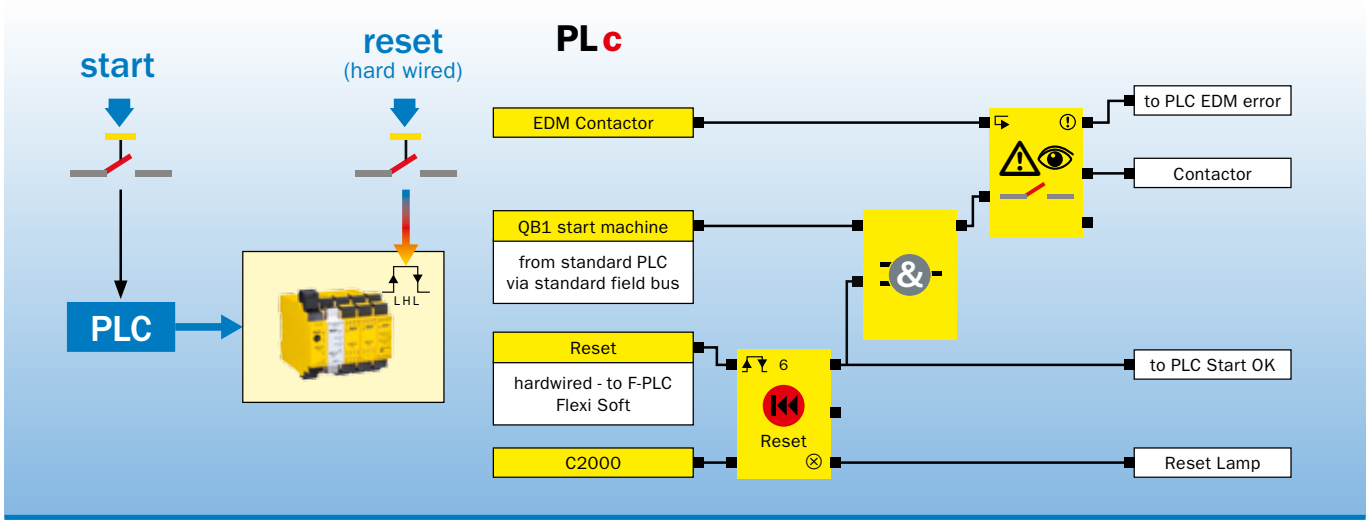
Een andere, vaak toegepaste reset is een hardwired knop waarvan het signaal via een standaardbus wordt verzonden naar de PLC en vandaar naar de veiligheidsbesturing. Tot nu toe werd algemeen aangenomen dat je een reset mocht laten meelopen in een standaardbesturing. SICK meent echter dat de reset moet worden opgewaardeerd. Het is en blijft een veiligheidsfunctie. En als zodanig is de reset ook in de normen opgenomen. Pas daarom ook altijd veiligheidsprincipes toe. Nog te veel mensen zijn niet of nauwelijks bekend met de basisveiligheidsprincipes die worden geformuleerd in de EN 13849-2 – de norm waarin ook de beproefde veiligheidsprincipes en componenten zijn opgenomen. Als je deze principes op de juiste wijze toepast, kun je niet te maken krijgen met zoiets als een paperclip die tussen een startknop is gestopt. Zo'n truc werkt dan gewoonweg niet meer.

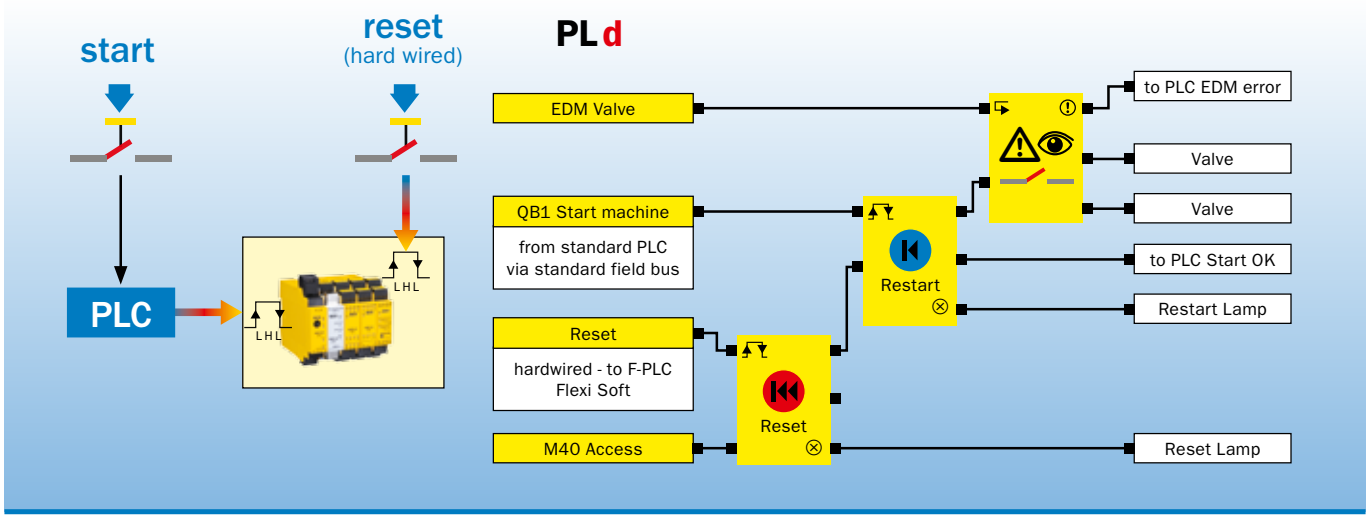
OPLOSSING DIE VERDER GAAT

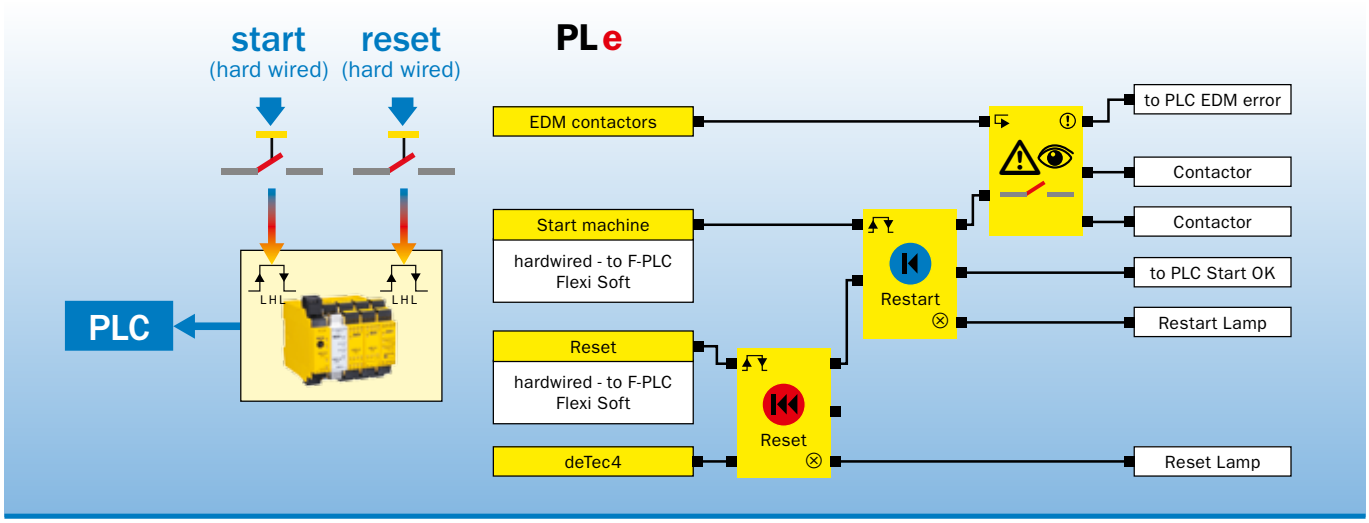
Volgens EN-13849-1 is de manuele reset een veiligheidsfunctie. Na de stopfunctie volgt doorgaans een manuele reset. Deze manuele reset moet geactiveerd worden door een manueel bediend component. Het mag alleen door een hoog-laagsignaal geactiveerd worden en mag niet per ongeluk geactiveerd kunnen worden.

SICK gaat iets verder. Aangezien de manuele resetfunctie eenkanalig is, heeft deze een Categorie 1-structuur. Volgens 13849-1 kun je daarbij in Performance Level nooit hoger komen dan PLc. Natuurlijk zijn er andere mogelijkheden om een hogere PL te bereiken. Maar de oplossing van SICK is: definieer de veiligheidsfunctie als 'voorkomen van onverwachts opstarten' of 'herstartblokkering'. Gebruik hierbij de reset en de start om een tweekanalige Categorie 3/4-structuur te realiseren. Zo kun je een hoger Performance Level bereiken.

Voor een PLd adviseert SICK minimaal een hardwired resetknop direct op het veiligheidscomponent of op de veiligheidsbesturing. Voor PLe luidt het advies: zowel de reset als de startknop hardwired direct op de veiligheidsbesturing. Op deze wijze kan de onderhoudsmonteur niet meer overvallen worden door een omvallend bitje, met een onverwachte herstart tot gevolg.







In dit schema vindt je de oplossing van SICK: definieer de veiligheidsfunctie als 'voorkomen van onverwachts opstarten' of 'herstartblokkering'. Gebruik de reset en de start voor een tweekanalige Categorie 3/4-structuur en een hoger Performance Level.

SICK
Sensor Intelligence.

SICK B.V. · Leijenseweg 111 · Postbus 186 · 3720 AD Bilthoven · Tel. 030 - 229 25 44 · Fax 030 - 229 39 94 · E-mail info@sick.nl · www.sick.nl