IEC 62443-3-2 "Security Systeem Ontwerp"

© *Rob Hulsebos*

Version 23/5/2023

Introductie

De norm IEC-62443 beschrijft hoe te werk moet worden gegaan om specifiek voor een industriële omgeving de cybersecurity in te regelen. Het is een voortzetting van de norm ISA-99 (de naam waaronder er nog vaak aan gerefereerd wordt). Die is al in 2007 uitgekomen, maar na de overdracht naar de IEC is fors doorgewerkt aan een verdere uitbouw. Bovendien is er na de uitbraak van de "Stuxnet" malware gekeken welke aanpassingen nodig waren om herhaling te voorkomen. Concreet vraagt de IEC 62443 om het inrichten van een "Information Security Management System" (ISMS) voor een "Industrial Automation and Control System" (IACS).

Van hoofdstuk 62443-3-2 "Security Risk Assessment and System Design" is begin 2018 de laatste versie uitgekomen, die nu (mei 2018) in stemming is. Het is een redelijk compact document, dat de workflow op een redelijk eenvoudige wijze beschrijft.

Zone & Conduit Requirements

De titel "Security Risk Assessment and System Design" geeft al aan dat in de IEC 63443-3-2 een belangrijke activiteit wordt uitgevoerd. Concreet: het definiëren van de beveiligingsmaatregelen om de cyber-risico's waaraan een IACS bloot staat tot een aanvaardbaar niveau terug te brengen. Welke risico's dat zijn, en wat "aanvaardbaar" is, en op welke wijze dat gehaald moet worden, wordt niet vastgelegd. Dat kan ook niet, want dat is immers de expertise van de IACS-eigenaar (asset owner).

Net zoals in de vorige versies van het document is er nog sprake van "Zones" en "Conduits":

- Een ***zone*** bevat alle assets (systemen, besturingen, netwerkapparatuur, software, I/O, etc.) waaraan gelijke beveiligingseisen worden gesteld.
- Een ***conduit*** bevat de communicatiekanalen tussen zones waaraan gelijke beveiligingseisen gesteld worden. Er kunnen dus meerdere conduits tussen 2 zones zijn.

De beveiligingsmethodiek van de IEC-62443 is dan zodanig dat de beveiligingsmaatregelen op de conduits geplaatst moeten worden, dus: overal waar data een zone ingaat of uitgaat. Dat hoeft dan niet persé een bekabeld netwerk te zijn: ook draadloze netwerken, mobiele verbindingen, etc. tellen ook mee. En: conduits-te-voet ook! Denk hierbij aan een medewerker die bestanden via een

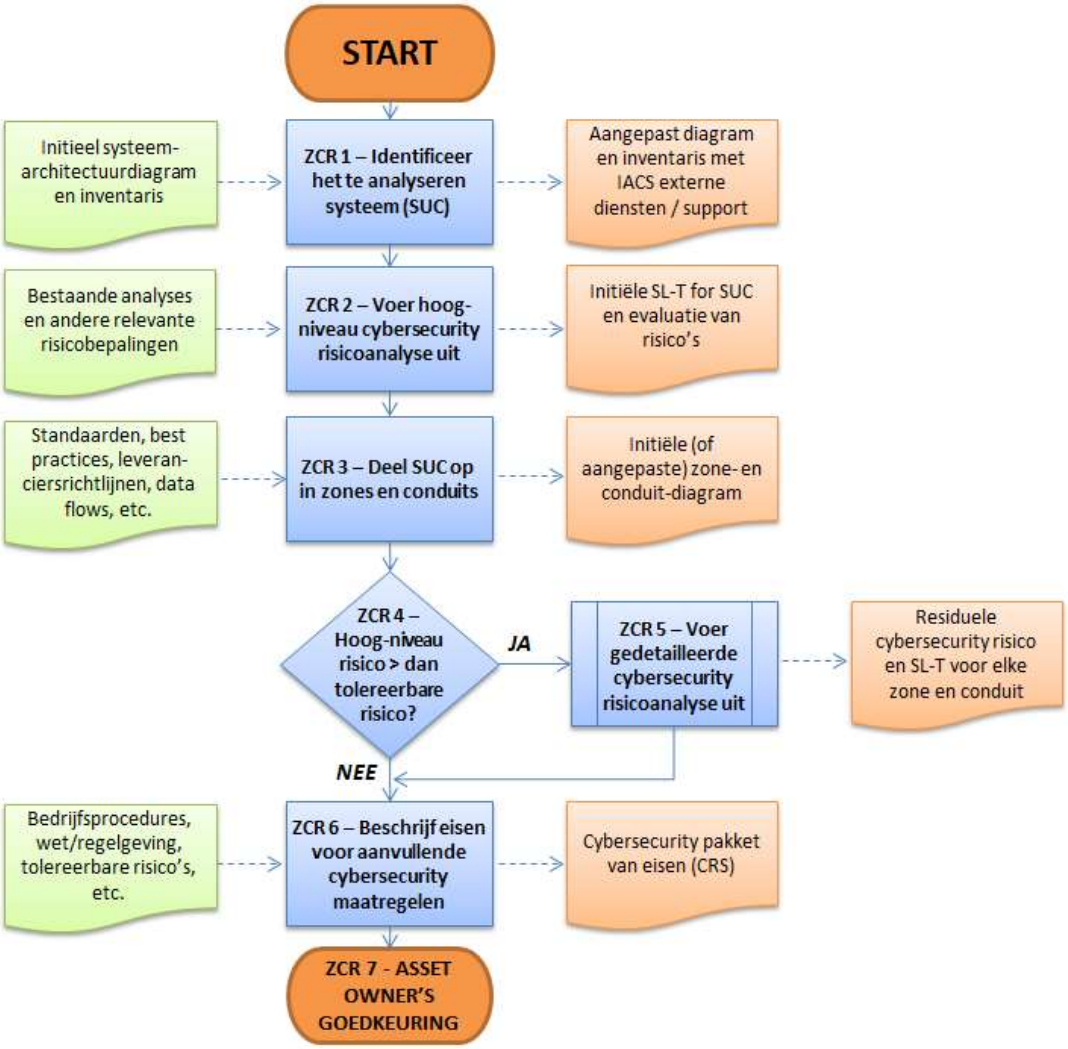
USB-stick van een apparaat in de ene zone naar een apparaat in een andere zone verplaatst[1]. Denk hierbij bijvoorbeeld aan een desktop-PC die verbinding heeft met internet, en een industriële PC in een productielijn.

Dat klinkt simpel genoeg, maar: *hoe* worden die zones en conduits dan bepaald? Daartoe is de 3-2 in zeven hoofdstukken onderverdeeld, getiteld:

- ZCR-1 Identificeer het te analyseren system ("SUC" – System Under Consideration)
- ZCR-2 Voer een hoog-niveau risicoanalyse uit
- ZCR-3 Deel SUC op in zones en conduits
- ZCR-4 Bepaal of het hoog-niveau risico acceptabel is
- ZCR-5 Voer een gedetailleerde cybersecurity risicoanalyse uit (optioneel)
- ZCR-6 Beschrijf eisen voor aanvullende cybersecurity maatregelen
- ZCR-7 Verkrijg toestemming van de asset-eigenaar

Deze lijst is op zich niet zo bijzonder, het is redelijk gezond boerenverstand, bijvoorbeeld ZCR-1, "Bepaal over welk systeem we het gaan hebben" en dan ZCR-2 "Hoe kwetsbaar zijn we".

Het volgende stroomschema geeft aan hoe de werkprocedure is, welke informatiebronnen / documenten / etc. (links) gebruikt kunnen worden, en welke documenten resulteren (rechts).



Per ZCR ("Zone and Conduit Requirements") zijn dan weer deelstappen beschreven, respectievelijk 1, 1, 6, 1, 13, 6 en 1. Hiervan is dan steeds beschreven wat gedaan moet worden (maar niet *hoe*).

[1] *Het risico van USB dient niet onderschat te worden, maar een verdere bespreking hiervan valt buiten het bereik van dit artikel. Meer informatie is wel te vinden op: www.enodenetworks.com/assets/docs/ProtectingAgainstUSBMalware.pdf.*

Dat kan natuurlijk ook niet, want elk IACS is anders, net zoals elk bedrijf, de risico's waaraan men blootstaat, en de consequenties van als het fout gaat. Er wordt ook geen technologie benoemd, die wijzigt immers zo snel dat als dit in de norm zou staan, deze in een paar jaar verouderd zou zijn.

In de tekst wordt steeds uitgelegd *waarom* een bepaalde deelstap nodig is. Dat helpt bij het begrijpen van de noodzaak van een dergelijke stap.

Een deelstap kan in een paar regels beschreven zijn, maar desondanks best veel werk betekenen. Een voorbeeld is ZCR-2.1 "Voer een hoog-niveau cybersecurity risicoanalyse uit", beschreven in slechts 4 regels. Maar in de analyse moet met alle mogelijke risico's rekening gehouden worden, culminerend in een risicomatrix waaruit dan een "Security Level Target" (gewenst beveiligingsniveau) komt rollen. Dit is dan weer bepalend voor te nemen vervolgstappen en de zwaarte van de te nemen beveiligingsmaatregelen.

Andere deelstappen zoals ZCR-3.5 "Separate wireless devices" zijn sneller te doen, namelijk het definiëren van aparte zone(s) voor draadloze apparatuur.

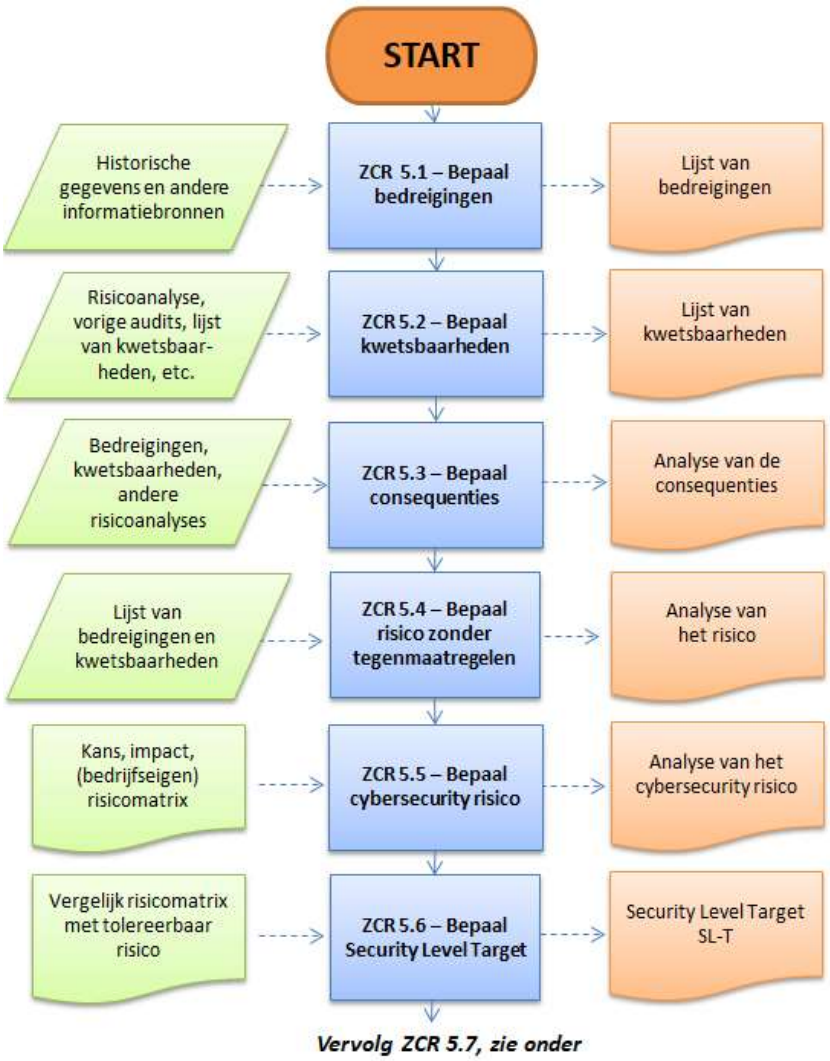
Eenmaal in ZCR-4 volgt een belangrijke beslissing: zijn de bestaande risico's acceptabel? Indien wel, dan hoeft geen gedetailleerde analyse meer gedaan te worden (in ZCR-5). Indien de risico's te hoog zijn, dan gaan we verder met ZCR-5, die zoveel werk omvat dat hiervoor een apart stroomschema is gemaakt (reden waarom hierboven ook het "Subroutine" symbool voor ZCR-5 is gebruikt).

De belangrijkste stap: ZCR-5

Indien de risico's *niet* acceptabel zijn, dan volgt in ZCR-5 het meeste werk. In maar liefst 13 stappen moeten de volgende activiteiten worden uitgevoerd:

- ZCR 5.1 Bepaal de bedreigingen
- ZCR 5.2 Bepaal de kwetsbaarheden
- ZCR 5.3 Bepaal de consequenties
- ZCR 5.4 Bepaal de kans op een bedreiging
- ZCR 5.5 Bepaal risico zonder gebruik van tegenmaatregelen
- ZCR 5.6 Bepaal "Security Level Target" (SL-T)
- ZCR 5.7 Is het risico acceptabel?
- ZCR 5.8 Bepaal bestaande cybersecurity tegenmaatregelen
- ZCR 5.9 Her evalueer kans & impact
- ZCR 5.10 Bepaal het residuele risico
- ZCR 5.11 Zijn alle residuele risico's acceptabel?
- ZCR 5.12 Bepaal additionele cybersecurity tegenmaatregelen
- ZCR 5.13 Documenteer en communiceer de resultaten

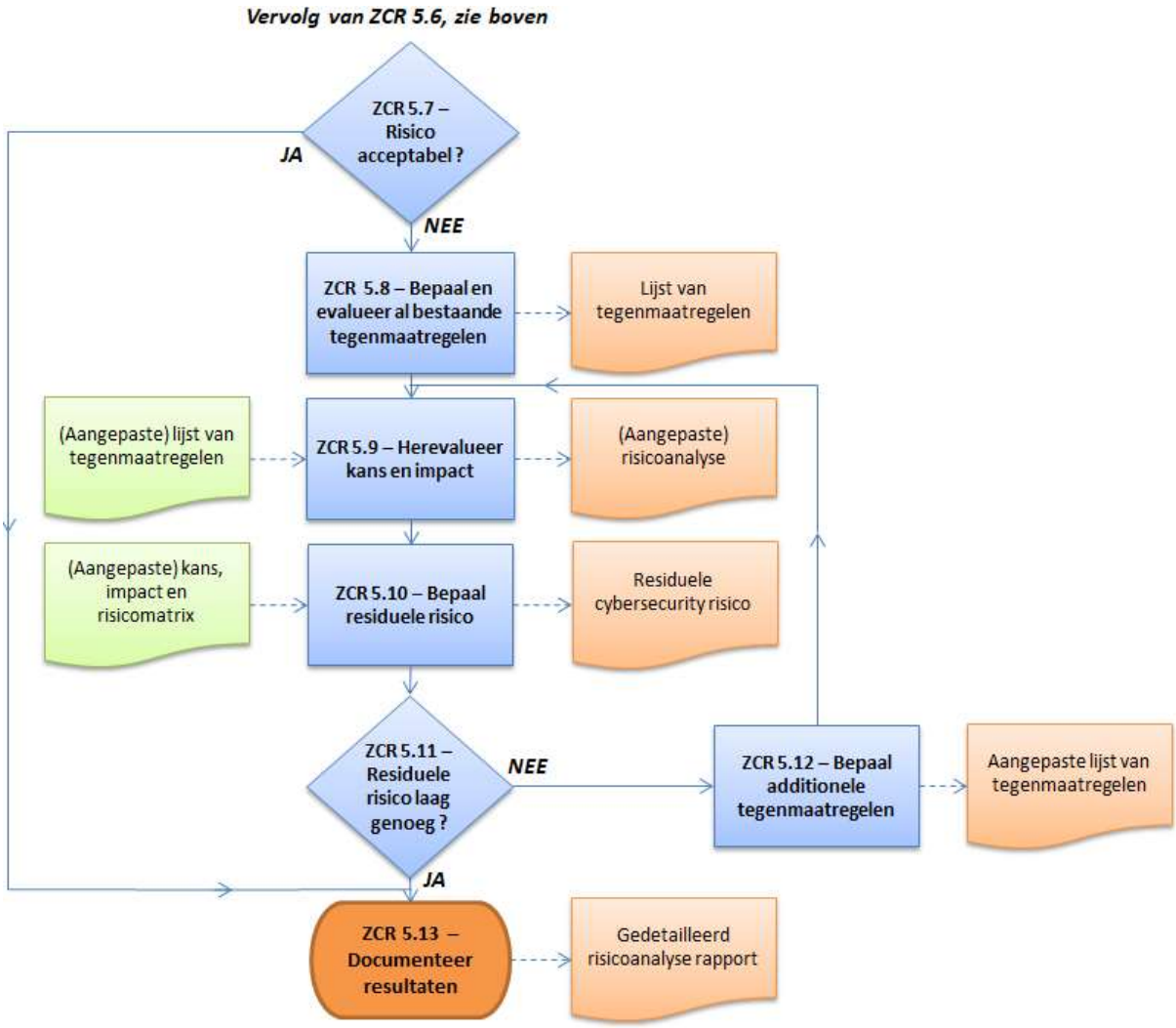
Ook hier is het werkproces beschreven in een stroomdiagram (dat hier in 2 delen wordt weergegeven). De eerste zes activiteiten ZCR 5.1 ... 5.6 zijn:



Het lijkt redelijk simpel, maar is het niet. Aan welke bedreigingen staat men bloot? Wat gebeurt er dan? En hoe hoog is de kans erop? Dit gaat niet enkel over cybersecurity, het is eigenlijk in ieder geval wel goed om er globaal eens over na te denken wat er allemaal zou kunnen gebeuren en welke impact dat heeft. Maar dat is voor nu verder niet van belang, de IEC 62443 kijkt enkel naar de cybersecurity.

Er wordt niet voorgeschreven welke risicoanalyse-methodologie moet worden gebruikt, zoals (bijvoorbeeld) ISO 31000, NIST SP800-39 of ISO 27005. In het IEC-document wordt (als inleiding) in een appendix nog wat uitgebreider ingegaan op wat een risicomatrix is en hoe daarmee omgegaan moet worden.

Na stap ZCR 5.6 wordt pas verder uitgewerkt welke beveiligingsmaatregelen eventueel nodig zijn. Misschien hoeft er helemaal niets gedaan te worden, als de risico's laag genoeg zijn, de kans erop ook heel laag en de schade ook beperkt blijft. Anderzijds kan men de risico's zo hoog inschatten, evenals de kans en de schadepost, dan moet onevenredig veel in tegenmaatregelen geïnvesteerd worden. De gulden middenweg is om te bepalen welk risico nog acceptabel is. Dit wordt in stap ZCR 5.7 bepaald. Indien de risico's te hoog zijn moet bedacht worden welke tegenmaatregelen noodzakelijk zijn om het risico lager te krijgen, net zolang tot het residuele risico wel acceptabel is. Dit kan dus betekenen dat meerdere keren stappen 5.9 t/m 5.12 moeten worden herhaald.



Uiteindelijk wordt afgesloten met stap 5.13, waarin de resultaten worden gedocumenteerd. Hiermee is dan een belangrijke fase afgerond, waarna teruggegaan wordt naar het hoofd-stroomschema (en de feitelijke implementatie kan beginnen).

Appendices

Het normdocument legt in 2 appendices nog uit wat een risicomatrix is, en wat "security-levels" (afkorting SL) zijn. Dit laatste begrip komt uit de IEC 62443-3-3, en verdient wat nadere uitleg.

Een SL wordt opgegeven als een getal met de waarde 0 t/m 4; hoe hoger de waarde des te zwaarder de beveiligingseisen:

- SL 0: geen specifieke beveiligingseisen, of geen beveiliging nodig.
- SL 1: bescherming tegen toevallig optredende inbreuken.
- SL 2: bescherming tegen opzettelijke inbreuk op de veiligheid, met gebruik van eenvoudige middelen, generieke vaardigheden of lage doelgerichtheid.
- SL 3: bescherming tegen opzettelijke inbreuk op de veiligheid, met gebruik van complexere middelen, IACS-specifieke kennis en vaardigheden, en gemiddelde doelgerichtheid.

- SL 4: bescherming tegen opzettelijke inbreuk op de veiligheid, met gebruik van geavanceerde hulpmiddelen, IACA-specifieke kennis en vaardigheden, en hoge doelgerichtheid.

In de IEC 62443-3-3 worden drie types security level (SL) vastgesteld:

Met "SL-T" (Security Level **Target**) stelt de asset-eigenaar of systeemintegrator vast aan welke niveau van beveiliging een bepaalde zone, systeem of component **moet** voldoen om een correcte werking te kunnen garanderen.

Met "SL-A" (Security Level **Achieved**) wordt het huidige beveiligingsniveau van een zone, systeem of component vastgelegd. Dit is nodig om te bepalen of de SL-T gehaald is.

Met "SL-C" (Security Level **Configured**) wordt vastgelegd welk SL een component of system kan halen als het op de juiste manier geconfigureerd / ingesteld is, zonder dat verdere maatregelen nodig zijn.

Uiteraard wordt als eerste de SL-T bepaald (zie ZCR-2 en ZCR-5). Daarna wordt bepaald welke maatregelen genomen moeten worden om hieraan te voldoen; van de oplossing wordt de SL-A bepaald, en als die lager is dan de SL-T is nog een iteratie nodig. Een onderdeel van dit werk is het selecteren (inkopen) van componenten (hardware, software), en de door de leverancier opgegeven SL-C bepaalt dan welke additionele maatregelen ("compensating controls") nog nodig zijn – hoe lager de SL-C, des te meer men zelf moet doen.

Meewerken?

IEC-normen worden geschreven door de deelnemende landen, die lokale vertegenwoordigers hebben. In Nederland is dat NEN (www.nen.nl), die over het vakgebied "Industrieel meten, regelen en automatiseren" normcommissie NEC65 opgesteld heeft. Deze normcommissie is binnen Nederland verantwoordelijk voor normen op het gebied van systemen en apparatuur voor besturing en bewaking van productieprocessen en industriële installaties.

Binnen de normcommissie NEC65 is weer het "Industrieel Platform Cybersecurity" (IPCS) actief. De leden hiervan komen 2x per jaar bijeen om kennis uit te wisselen over nieuwe ontwikkelingen op het gebied van cybersecurity, en dragen ook bij aan de invulling van de IEC 62443. Lidmaatschap staat voor iedereen open; meer informatie is te vinden op: www.nen.nl/Normontwikkeling/energy/Industrieel-Platform-Cyber-Security.htm