Ministerie van Justitie en Veiligheid

IACS Coalitie werkgroep

Publicatie Crisismanagement

Oktober 2025

IACS Coalitie

Inhoud

Inleiding

Het belang van goed IACS-beheer en crisismanagement is groot. Uitval van IACS kan namelijk leiden tot maatschappelijke onrust, reputatieschade, gevaarlijke situaties en verstoring van vitale processen. Dit vraagt om het in kaart brengen van systemen, het analyseren van risico's en het opstellen van plannen om snel en effectief te reageren op storingen of incidenten. Daarbij is er een sterke link met veiligheid, gezondheid en milieu (HSE), omdat veel IACS-systemen invloed hebben op de fysieke leefomgeving

Deze onderwerpen zijn relevant voor een breed publiek. Overheden gebruiken IACS bijvoorbeeld in verkeerssystemen, waterbeheer en gebouwbeheersystemen. Bedrijven en de industrie vertrouwen erop voor hun productie, logistiek en energiebeheer. Voor beleidsmakers, beheerders, veiligheidsprofessionals en IT-specialisten is het begrijpen en beheren van IACS van groot belang om risico's te beperken en de samenleving en economie veerkrachtig te houden. Daarnaast speelt wetgeving en compliancy een rol, denk alleen maar aan de NIS2/cyberbeveiligingswet (Cbw) en de Cyber Resilience Act (CRA).

In deze publicatie hebben we het over IACS, ook worden andere termen gebruikt om IACS te duiden, bijvoorbeeld OT – Operationele technologie wat de tegenhanger is van IT. Zie ook: Wat is IACS?

Doelgroep

Doelgroep is MKB, overheid en bedrijven die niet zelfstandig in staat zijn grote programma's op het gebied van cyberweerbaarheid van IACS uit te voeren. Daarmee is dit document een praktische handleiding voor IACS-crisismanagement.

Deze publicatie is gemaakt door de IACS Coalitie in samenwerking met

Thales en Accenture

Samenvatting

Industrial Automation and Control Systems (IACS) zijn cruciale systemen die fysieke processen automatisch en veilig aansturen. Deze processen hebben vaak een grote maatschappelijke waarde. Het is daarom van belang om plannen op te stellen om snel en effectief te reageren op storingen of incidenten aan deze processen.

Risico's van IACS-uitval

IACS-uitval kan leiden tot grote maatschappelijke gevolgen, zoals verkeerschaos, wateroverlast, reputatieschade, gevaarlijke situaties, en verstoring van vitale processen. Hierdoor is het essentieel dat IACS goed worden beheerd en dat er effectieve crisismanagementplannen aanwezig zijn.

Strategieen voor IACS Crisismanagement

Hieronder is een stappenplan omschreven om een start te maken met crisismanagement:

1. **Inventarisatie en Classificatie van IACS-systemen**
   - Bepaal welke IACS-systemen aanwezig zijn en wat hun functies zijn;
   - Classificeer deze systemen op basis van hun invloed op kernprocessen en potentiële risico's van uitval of verstoring.

2. **Risicoanalyse en Crisisplannen**
   - Identificeer wat er mis kan gaan (storingen, cyberaanvallen, etc.) en wat de mogelijke gevolgen dan zijn;
   - Ontwikkel duidelijke crisisplannen voor deze systemen, met vastgelegde verantwoordelijkheden en maatregelen om schade te beperken.

3. **Regelmatig Oefenen**
   - Test crisisplannen regelmatig met realistische scenario's;
   - Identificeer zwakke punten in de plannen en verbeter waar nodig.

4. **Integratie met HSE (Health, Safety, and Environment)**
   - Zorg ervoor dat IACS-crisismanagement geïntegreerd is met bredere HSE-processen;
   - Dit omvat ten minste veiligheid, gezondheid, en milieubeheer tijdens noodsituaties.

Voordelen van een Robuust IACS-crisismanagement

- **Minimale maatschappelijke schade:** beperkt de impact van IACS-uitval op het dagelijks leven, de economie en infrastructuur;
- **Verbeterde veiligheid:** zorgt voor een veiligere werkomgeving en beschermt het milieu;
- **Betere reputatie:** voorkomt reputatieschade door bewezen beheer en snelle respons tijdens incidenten;
- **Compliance:** voldoet aan nationale en internationale HSE-regelgevingen en cybersecurity wetten.

Aanbevelingen voor MKB en overheid

1. **Inventarisatie en classificatie:** begin met het in kaart brengen van alle IACS-systemen en hun functies. Bepaal, al dan niet met je leverancier, de prioriteiten voor onderhoud en beveiliging;
2. **Risicoanalyse en crisisplannen:** voer grondige risicoanalyses uit en stel crisisplannen op voor vitale systemen;
3. **Oefenen en updaten:** test de crisisplannen regelmatig, evalueer de resultaten, en werk deze bij naar aanleiding van nieuwe risico's en omstandigheden;
4. **Integratie met HSE:** zorg voor een geïntegreerd beheer dat verbinding maakt tussen technische, operationele, HSE-aspecten en ICT-beheer.

Door deze stappen te volgen, zet je een robuust systeem op voor IACS-beheer en crisismanagement, waarmee je zowel de veiligheid als de continuïteit van vitale processen waarborgt.

Wat is IACS?

IACS zijn systemen die ervoor zorgen dat alledaagse dingen soepel en veilig verlopen, zoals het schakelen van verkeerslichten, het aansturen van rioolgemalen, of het regelen van de temperatuur in een gebouw. Je kunt ze zien als de slimme regelapparatuur die ervoor zorgt dat de wereld om ons heen functioneert zonder dat we er actief over na hoeven te denken. IACS maakt het mogelijk dat bijvoorbeeld bruggen automatisch openen voor schepen, tunnels veilig blijven voor verkeer, en zwembaden comfortabel warm zijn en dat complexe industriële toepassingen worden uitgevoerd.

Wat IACS zo interessant maakt, is de enorme variatie in schaal en complexiteit. Een IACS-systeem kan heel klein en eenvoudig zijn, zoals een enkele sensor die de temperatuur in een ruimte meet en een kachel aanstuurt. Maar het kan ook een enorm complex systeem zijn, zoals in een petrochemisch bedrijf, waar talloze processen en machines met elkaar samenwerken om olieproducten te raffineren.

Tussen deze uitersten vind je talloze voorbeelden, zoals verkeerslichten, gebouwenbeheersystemen, camerasystemen voor veiligheid, of waterzuiveringsinstallaties. Deze systemen zijn overal om ons heen en spelen een cruciale rol in ons dagelijks leven. Ondanks dat we ze vaak niet bewust opmerken, zouden veel dingen zonder IACS simpelweg niet werken.

Verschil met IT

Het grote verschil met IT is dat IACS zich richt op het aansturen van fysieke processen, terwijl IT draait om het verwerken en beheren van informatie, zoals e-mails of documenten. Waar IT vaak flexibel en snel aan te passen is, zijn IACS-systemen ontworpen om jarenlang betrouwbaar te functioneren, soms wel tientallen jaren. Hierdoor gebruiken ze vaak oudere technologie die lastig te updaten is. Daarnaast kent IACS ook netwerktechnologie die steeds vaker wordt toegepast. Dit maakt ze extra kwetsbaar voor storingen en cyberaanvallen, wat een groot risico inhoudt, vooral bij kritieke processen.

IACS bij de overheid

De overheid maakt gebruik van een breed scala aan IACS-systemen, die zowel op lokaal, regionaal als landelijk niveau worden ingezet om cruciale processen in de fysieke wereld te beheren. Enkele voorbeelden van dergelijke systemen zijn:

- Verkeersregelinstallaties (VRI's), in de volksmond stoplichten
- Rioolpompgemalen
- Gebouwbeheersystemen
- Fysieke toegangsbeheersystemen
- Camerasystemen
- Verlichting van openbare wegen
- Brug- en sluisbedieningssystemen
- Weegbruggen
- Tunnelsystemen
- Waterbeheerinstallaties
- Openbare laadinfrastructuur
- Parkeersystemen
- Slimme afvalinzamelingssystemen
- Luchtkwaliteits- en milieumonitoringsystemen
- Vaarwegverlichting en nautische signalering

Deze IACS-systemen spelen een essentiële rol in het functioneren van de openbare ruimte en infrastructuur. Ze maken het leven veiliger, efficiënter en duurzamer en zijn onmisbaar voor een goed functionerende samenleving.

IACS bij de industrie

In bedrijven en de industrie worden IACS veelvuldig toegepast om processen te automatiseren en efficiënter te maken. Deze systemen kunnen variëren van kleine, specifieke oplossingen tot grote complexe installaties. Hier zijn enkele veelvoorkomende voorbeelden van IACS in het bedrijfsleven en de industrie:

- Productielijnen in fabrieken
- Medische apparatuur
- Energiecentrales
- Procescontrole in de petrochemische industrie
- Koel- en vriesinstallaties
- Opslagtanksystemen
- Automatische magazijnen en logistieke systemen
- CNC-machines in metaal- en houtbewerking
- Drukkerijen
- Gebouwbeheersystemen
- Beheersystemen voor datacenters
- Brouw- en bottelinstallaties
- Mijnbouwapparatuur
- Papier- en pulpindustrie
- Verf- en coatinginstallaties
- Afvalverwerkingsinstallaties
- Farmaceutische productiefaciliteiten
- Waterzuiveringsinstallaties
- Transportbanden en sorteersystemen
- Booreilanden
- Glas- en keramiekproductie

Deze systemen spelen een cruciale rol in het verhogen van de efficiëntie, het waarborgen van kwaliteit en het verlagen van kosten in de industrie. Ze zijn vaak de stille kracht achter de meeste producten en diensten die we dagelijks gebruiken.

Beheersing

Als een IACS-systeem uitvalt, kunnen de gevolgen groot zijn, omdat deze systemen vaak verantwoordelijk zijn voor het soepel laten verlopen van processen die we als vanzelfsprekend beschouwen. Als bijvoorbeeld verkeerslichten niet meer werken, ontstaat chaos op de weg met mogelijke ongelukken tot gevolg. Wanneer rioolpompen uitvallen, kan dat leiden tot vervuiling, wateroverlast of zelfs overstromingen. En als een gebouwbeheersysteem niet goed functioneert, kunnen mensen in een kantoor of ziekenhuis last krijgen van slechte ventilatie, kou of hitte.

Uitval van IACS kan ook zorgen voor maatschappelijke onrust. Denk aan het stilvallen van bruggen en tunnels, waardoor duizenden mensen vast komen te staan. Of de storing van camera- en veiligheidssystemen, waardoor burgers zich onveilig voelen. In sommige gevallen kan uitval leiden tot gewonden of zelfs levensgevaarlijke situaties, bijvoorbeeld als een fabriek niet meer veilig kan worden stilgelegd of als een stroomuitval ziekenhuizen en vitale diensten raakt.

Daarnaast brengt uitval vaak een afbreukrisico met zich mee. Overheden en bedrijven kunnen reputatieschade oplopen als blijkt dat systemen niet goed zijn onderhouden of onvoldoende zijn beveiligd. Dit leidt tot negatieve publiciteit en een verlies van vertrouwen bij burgers of klanten. Bijvoorbeeld, als blijkt dat een cyberaanval op een waterzuiveringsinstallatie het drinkwater heeft besmet, is de maatschappelijke impact enorm.

Bovendien kan uitval van IACS maatschappelijke processen verstoren. Stel je voor dat het stroomnetwerk van een stad platligt of dat een afvalverwerkingsinstallatie wekenlang niet functioneert. Dit heeft directe gevolgen voor het dagelijks leven, de economie en de infrastructuur.

Om dit soort risico's te beheersen, is het belangrijk om IACS-systemen goed te classificeren in relatie tot het effect op de kernprocessen. Dit betekent dat je bepaalt hoe belangrijk een systeem is en wat de gevolgen zouden zijn als het uitvalt. Bijvoorbeeld, een systeem dat een tunnel veilig houdt, heeft een hogere classificatie nodig dan een systeem dat alleen verlichting in een kantoor regelt. Deze classificatie helpt prioriteiten te stellen voor onderhoud, beveiliging en herstel in geval van uitval.

Beheerprocessen zijn cruciaal om IACS-systemen veilig en betrouwbaar te houden. Het gaat er niet alleen om storingen te voorkomen, maar ook om voorbereid te zijn op noodsituaties. Daarom is IACS-crisismanagement zo belangrijk. Dit omvat plannen en processen om snel en effectief te reageren op storingen of aanvallen. Door goed crisismanagement kunnen de gevolgen van een incident worden beperkt en kan een systeem zo snel mogelijk weer operationeel zijn, zodat maatschappelijke schade en onrust worden geminimaliseerd. Voorkomen is beter dan genezen. Ook hier.

IACS Crisismanagement - handelingsperspectief

Het goed beheren en classificeren van IACS is van groot belang. Evenals het maken van plannen voor storingen en incidenten zodat je die snel en effectief kunt oplossen. Dit noemen we IACS-crisismanagement. Om goed IACS-crisismanagement op te zetten, doorloop je vier stappen.

Stap 1: Inventarisatie en classificatie van IACS-systemen

Begin met een volledig overzicht van alle aanwezige IACS-systemen en bepaal hoe belangrijk elk systeem is en wie ervoor verantwoordelijk is. Dit geeft je een overzicht van alle systemen en maakt het mogelijk om te bepalen welke als cruciaal worden beschouwd, bijvoorbeeld een systeem dat een rioolpompgemaal of verkeerslichten aanstuurt. Dit helpt om prioriteiten te stellen en inzicht te krijgen in waar risico's het grootst zijn en wie het aanspreekpunt is.

Stap 2: Opstellen van risicoanalyses en crisisplannen

Analyseer wat er mis kan gaan zoals (ver)storingen, cyberaanvallen of menselijke fouten, en wat de mogelijke gevolgen daarvan zijn. Op basis van deze risicoanalyse maak je een classificatie, waarbij je vaststelt hoe belangrijk een systeem is en hoeveel aandacht het verdient. Systemen met directe invloed op veiligheid of vitale processen krijgen een hogere prioriteit. Ontwikkel voor cruciale systemen duidelijke crisisplannen die beschrijven wie verantwoordelijk is, wat er moet gebeuren, en hoe schade wordt beperkt. Voor elk belangrijk systeem stel je vervolgens een crisisplan op. Ook communicatie speelt hierin een belangrijke rol: het plan beschrijft wie op de hoogte moet worden gesteld en hoe informatie effectief wordt verspreid.

Stap 3: Oefenen en updaten

Test de crisisplannen regelmatig met realistische scenario's om te zorgen dat iedereen weet wat te doen. Werk deze plannen bij naarmate risico's of systemen veranderen. Door scenario's te testen wordt duidelijk of de plannen werken en of iedereen weet wat er in geval van een verstoring (incident) moet gebeuren. Hierbij kun je zwakke plekken ontdekken en verbeteren. Tot slot wil je de plannen en processen beheren en bijwerken, zodat ze blijven aansluiten op veranderende risico's en omstandigheden, zelfs als de technologie van veel IACS-systemen relatief stabiel blijft.

Stap 4: Integreren met HSE en bredere crisisprocessen

IACS-crisismanagement vertoont overeenkomsten met andere vormen van beheer en crisismanagement. Net als bij IT-beheer werk je met overzicht, monitoring en snelle reactie op incidenten. Ook met bedrijfscrisismanagement zijn parallellen te trekken, zoals het voorkomen van verstoringen en het managen van noodsituaties via plannen en oefeningen. Daarnaast zijn er raakvlakken met fysieke veiligheids(safety)processen, omdat veel IACS-systemen direct gerelateerd zijn aan fysieke veiligheid, bijvoorbeeld systemen die fabrieken stilleggen bij een noodsituatie of zorgen voor veilige tunnelomstandigheden.

De relatie met HSE (Health, Safety, and Environment) is eveneens belangrijk. Veel IACS-systemen hebben een directe invloed op gezondheid, veiligheid en milieu. Ze regelen bijvoorbeeld ventilatie en luchtkwaliteit, bewaken veilige productieprocessen en beheren systemen voor waterzuivering en energie-efficiëntie. Door HSE te integreren in IACS-crisismanagement beheers je niet alleen technische risico's, maar besteed je ook aandacht aan de impact op mensen en de omgeving. Dit draagt bij aan een betere voorbereiding op incidenten en minimaliseert de mogelijke gevolgen: door HSE-maatregelen kan bijvoorbeeld de bedrijfsvoering door de veiligheidsregio stilgelegd worden.

Bijlagen

Bijlage 1: Inventarisatie en classificatie van IACS

Bij de inventarisatie en classificatie van Industrial Automation and Control Systems (IACS) is het essentieel om een gedetailleerd scenario te ontwikkelen voor digitale uitval. Deze scenario zijn de basis voor de operationele risico's van een asset. Daarnaast is het goed te realiseren dat cybersecurity van assets begint bij de aanschaf.

Objectclassificatie is een combinatie van directe afhankelijkheid van het geïsoleerde object in combinatie met een totale keten van afhankelijkheden. Belangrijk is op te nemen wanneer in de tijd een defect object een probleem ontstaat. Geclassificeerde Objecten moet je jaarlijks toetsen.

De Cybersecurity Implementatierichtlijn Objecten (CSIR) van de Rijkswaterstaat CIV/IRN/Security Centre/Security by Design en Het Waterschapshuis geeft gedetailleerde handvatten te vinden bij CERT-WM: CSIR pagina bij CERT-WM

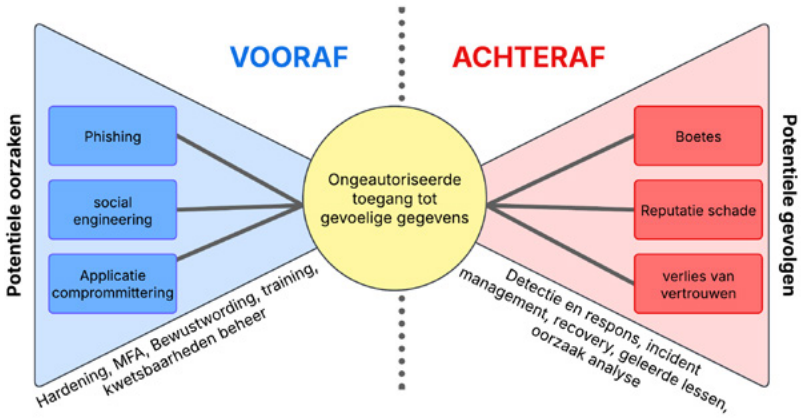
De risico-inventarisatie start bij de aanschaf, aangezien het kiezen van de juiste componenten en leveranciers een directe invloed kan hebben op de algehele beveiligingspositie. Vanaf het begin moet de nadruk liggen op de juiste oplossing die rekening houdt met de functionele en niet-functionele beveiligings- en safety-eisen = en dus niet op de goedkoopste oplossing. Ga zorgvuldig om met deze initiële fase. Doe je dat niet, dan kan dit leiden tot aanzienlijke operationele verstoringen en veiligheidsproblemen in de toekomst.

Leg tijdens de verwerving de nadruk op de noodzaak om te beginnen met het verzamelen van informatie over de Software Bill of Materials (SBOM) en de Bill of Materials (BOM). Dit is belangrijk omdat hierover later ook kwetsbaarheidswaarschuwingen worden gegeven die van belang zijn bij het veilig houden gedurende de levensduur van het object.

Daarna is het van belang om een gestructureerde aanpak te hanteren bij de inventarisatie, classificatie en het risicomanagement van IACS-systemen. Deze gegevens zijn cruciaal voor het identificeren van kwetsbaarheden die kunnen voortvloeien uit het gebruik van specifieke componenten. Het beheer van kwetsbaarheden is een doorlopend proces dat niet alleen de identificatie van risico's omvat, maar ook de impact van de apparaten op de operationele processen van de organisatie.

Een voorbeeld van gestructureerde risico analyse is het BowTie model

Een BowTie in risicomanagement is een visuele scenario-gebaseerde methode voor risico-identificatie, -analyse en -management . Het model vereenvoudigt elke gevaarlijke realiteit zonder deze te oversimplificeren en helpt de integriteit van barrières te behouden. De BowTie-methode structureert de voornaamste risico's van de organisatie en geeft een duidelijk overzicht van de manier waarop deze worden beheerst. De barrières in het BowTie-diagram laten beheersmaatregelen in het managementsysteem zien die ongewenste consequenties moeten voorkomen, mitigeren of elimineren.



Bijlage 2: Opstellen van risicoanalyse en crisisplannen

Opstellen risicoanalyses

In het kader van risicobehandeling is het essentieel om de diverse belangen af te wegen van risico's tegen de risicobereidheid (hoeveel risico kan en wil een organisatie nemen) van de organisatie. Dit betekent dat de organisatie zelf bepaalt hoeveel risico zij bereid is te dragen. Om dit adequaat te doen is het van belang om vast te stellen welke IACS-componenten de organisatie in huis heeft en welke daarvan van belang dan wel nodig zijn voor de kritieke processen. En waar nodig (extra) maatregelen te treffen waardoor de continuïteit beter gewaarborgd wordt.

Het doel van risicomanagement is om relevante risico's terug te brengen tot een niveau dat voor de organisatie acceptabel is. Daarbij weeg je af of er aanvullende maatregelen nodig zijn. Er zijn twee onderwerpen die specifiek aandacht vragen.

Risicoanalyse uitvoeren

- **Grote organisaties:** Voer een uitgebreide risicoanalyse uit, waarbij interne en externe risico's voor IACS worden geïdentificeerd. Dit kan inhouden dat er gebruik wordt gemaakt van risicobeoordelingsmodellen en het in kaart brengen van mogelijke scenario's, zoals cyberaanvallen, fysieke storingen, of natuurrampen.
- **Kleine organisaties:** Focus op het identificeren van de meest waarschijnlijke en impactvolle risico's. Gebruik eenvoudige tools of checklists om de belangrijkste bedreigingen te inventariseren.

Bedreigingsidentificatie uitvoeren

- Maak een lijst van potentiële bedreigingen specifiek voor IACS, zoals malware gericht op OT-systemen, stroomuitval, menselijke fouten, of technische storingen. Stel vast welke van deze bedreigingen van toepassing zijn voor de organisatie.

Door de onderkende risico's die van belang zijn voor de organisatie naast de potentiële bedreigingen te leggen, stelt dit een organisatie in staat om een goede afweging te maken wat de kans en de impact is van een onderkend risico. Op basis hiervan kan een organisatie een keuze maken hoe om te gaan met het onderkende risico. Door het doorlopen van onderstaande stappen maakt de risicobehandeling voor een organisatie haalbaar en herhaalbaar. Het zijn activiteiten die uitgevoerd moeten worden om tot een meer specifieke risicoanalyse en – uitkomsten te komen en op basis hiervan mogelijk maatregelen te definiëren.

De navolgende stappen worden onderkend bij de risicobehandeling

1. Wat is belangrijk voor de organisatie of wat zijn de **Te Beschermen Belangen** (TBB). Stel vast wat voor de organisatie van belang is als het gaat om IACS objecten binnen de organisatie.
2. Voer een **bedreigingenanalyse** uit specifiek voor IACS van zowel interne – als ook externe bedreigingen.
3. **Risico-acceptatie vs. mitigatie:** Organisaties moeten zelf bepalen of zij een risico accepteren, of dat zij maatregelen nemen om het risico te verminderen.
4. **Strategieën voor risicomitigatie:** Kies de meest geschikte strategie om het risico te beheersen, zoals vermijden, overdragen, verminderen of accepteren.
5. **Modelleren van de impact:** Beoordeel de verwachte effecten van de gekozen maatregelen.
6. **Implementatie van beheersmaatregelen:** De maatregelen uitvoeren en ervoor zorgen dat deze effectief aantoonbaar de impact van het risico doen verminderen of zelfs wegnemen.

Specifieke aandacht in relatie tot IACS is ook nodig voor HSE. HSE staat voor Health, Safety & Environment en verwijst naar het geheel van richtlijnen, beleidsmaatregelen en procedures die organisaties implementeren om de gezondheid en veiligheid van werknemers te waarborgen en de milieu-impact van hun activiteiten te minimaliseren.

De drie pijlers van HSE zijn:

1. **Gezondheid (Health)**
   - Bescherming van de fysieke en mentale gezondheid van werknemers.
   - Preventie van beroepsziekten door ergonomische werkplekken, medische controles en gezondheidsprogramma's.
2. **Veiligheid (Safety)**
   - Vermindering van werk gerelateerde risico's door veiligheidsprocedures en training.
   - Gebruik van persoonlijke beschermingsmiddelen (PBM's) en noodplannen om incidenten te voorkomen.
3. **Milieu (Environment)**
   - Duurzaam beheer van grondstoffen en energieverbruik.
   - Afvalbeheer en naleving van milieuwetgeving om negatieve impact te minimaliseren.

Hieronder volgt een aantal belangrijke en noodzakelijke aspecten van HSE, die voor een organisatie van belang zijn:

HSE aspecten

Veiligheidsintegratie in IACS

- **Safety Instrumented Systems (SIS)**: implementeer Safety Instrumented Systems die automatisch ingrijpen bij gevaarlijke omstandigheden om de veiligheid van het personeel en de omgeving te waarborgen. Deze systemen moeten regelmatig worden getest en onderhouden.
- **Functional Safety**: zorg ervoor dat IACS voldoen aan functionele veiligheidseisen zoals gedefinieerd in normen zoals IEC 61508 en IEC 61511, die zich richten op het reduceren van risico's tot een aanvaardbaar niveau.

Risicobeoordeling en Veiligheidsprotocollen

- **Risicoanalyse**: voer regelmatig risicobeoordelingen uit om potentiële gevaren te identificeren en adequate veiligheidsmaatregelen te implementeren. Dit omvat zowel technische risico's als operationele veiligheidsaspecten.
- **Veiligheidsprotocollen**: ontwikkel en implementeer duidelijke veiligheidsprotocollen die gericht zijn op het beschermen van medewerkers, apparatuur, en het milieu tijdens de werking van IACS.

Safety (Veiligheid)

Fail-Safe Mechanismen

- **Fail-Safe Systems**: ontwerp systemen die automatisch in een veilige modus gaan bij een storing. Dit kan inhouden dat systemen worden uitgeschakeld of naar een veilige toestand worden terug-gebracht om schade of letsel te voorkomen.
- **Safety Interlocks**: implementeer mechanische of softwarematige interlocks die voorkomen dat gevaarlijke acties worden uitgevoerd tenzij aan specifieke voorwaarden is voldaan.

Continual Safety Assessments

- **Periodieke Veiligheidsbeoordelingen**: voer regelmatig veiligheidsbeoordelingen en audits uit om de effectiviteit van bestaande veiligheidsmaatregelen te evalueren en deze waar nodig aan te passen of te verbeteren.
- **Testen van Noodprocedures**: oefen en test noodprocedures regelmatig met simulaties om ervoor te zorgen dat het personeel klaar is om effectief te reageren op veiligheidsincidenten.

Integratie van Cybersecurity en Safety

- **Security-Safety Convergence**: zorg voor een nauwe integratie van cybersecurity- en veiligheids-maatregelen om ervoor te zorgen dat cyberdreigingen geen fysieke veiligheidsrisico's kunnen veroorzaken. Dit houdt in dat zowel IT als OT (Operationele Technologie) teams samenwerken om risico's holistisch te beheersen.

Milieuoverwegingen

- **Milieubeheer en Compliance**: implementeer processen om ervoor te zorgen dat IACS voldoen aan milieuregels en dat operationele activiteiten de impact op het milieu minimaliseren, bijvoorbeeld door efficiënt energiebeheer en emissiereductie.
- **Milieu Monitoring**: gebruik IACS voor het continu monitoren van omgevingsfactoren zoals lucht- en waterkwaliteit om te voldoen aan milieuvoorschriften en om mogelijke incidenten vroegtijdig te detecteren.

Het verhogen van het risicobewustzijn en de continuïteit van IACS vereist een multidisciplinaire aanpak waarbij technische architectuur, operationele processen, HSE-aspecten, en veiligheid zorgvuldig worden geïntegreerd. Door redundantie en veerkracht in het ontwerp te bouwen, processen te optimaliseren, veiligheidsprotocollen strikt na te leven, en continue monitoring en evaluatie uit te voeren, verbeteren organisaties de continuïteit van hun IACS-systemen significant en tegelijkertijd de veiligheid van personeel en milieu waarborgen.

Crisismanagement en crisismanagementplan

Continuïteit en crisismanagement zijn essentieel om de operationele stabiliteit van een organisatie te waarborgen, vooral in omgevingen die afhankelijk zijn van IACS (Industrial Automation and Control Systems). Hieronder volgt hoe je kunt omgaan met continuïteit en crisismanagement.

Crisismanagement richt zich op de onmiddellijke reactie op en het beheer van een crisissituatie om de schade te beperken en de normale operaties zo snel mogelijk te herstellen.

Een crisismanagementplan helpt organisaties bij het voorbereiden, reageren en herstellen van crises. De kernpunten van zo'n plan zijn:

1. Risicoanalyse en scenarioplanning

- Identificeren van potentiële crises (bijv. natuurrampen, cyberaanvallen, financiële crises).
- Evalueren van de impact en waarschijnlijkheid van deze risico's.
- Opstellen van verschillende scenario's en bijbehorende responsstrategieën. Denk hierbij aan:
  - Schadebeperking; snelle evacuatie, tijdelijke afsluiting van systemen, eerste hulpverlening.
  - Afbakenen: isoleren van getroffen systemen bij een cyberaanval, beperken van communicatie om paniek te voorkomen.
  - Samenwerking; inschakelen van politie bij fysieke dreiging, samenwerken met cybersecurity-experts bij een datalek.
  - Continuïteit; werken vanuit een noodlocatie, inzetten van back-up IT-systemen, gebruik van noodvoorraad.

2. Crisisorganisatie en verantwoordelijkheden

- Benoemen van een *crisismanagementteam* (CMT) met duidelijke rollen (bijv. crisismanager, communicatieverantwoordelijke, IT-expert).
- Toewijzen van specifieke taken en verantwoordelijkheden.
- Inrichten van een *commandostructuur* voor snelle besluitvorming.

3. Communicatieprotocol

- Opstellen van een communicatieplan voor interne en externe belanghebbenden.
- Benoemen van woordvoerders en vaststellen van communicatielijnen.
- Gebruik van crisiscommunicatiekanalen zoals persberichten, sociale media en noodmeldingen.

4. Actie- en escalatieprocedures

- Stappenplan voor de eerste reactie op een crisis.
- Escalatiecriteria om te bepalen wanneer externe partijen (zoals overheid of hulpdiensten) moeten worden ingeschakeld.
- Procedures voor noodmaatregelen en bedrijfscontinuïteit.

5. Bedrijfscontinuiteit en herstelstrategieeen

- Plan voor het minimaliseren van onderbrekingen en hervatten van kritische bedrijfsprocessen.
- IT- en databeveiligingsmaatregelen, inclusief back-ups en alternatieve werkmethoden.
- Evaluatie- en verbeterprocedures na de crisis om het plan te optimaliseren.

Een effectief crisismanagementplan moet regelmatig worden getest en geüpdatet, zodat de organisatie goed voorbereid is op onverwachte gebeurtenissen.

Bijlage 3: Oefenen en updaten

Er zijn verschillende soorten oefeningen voor crisismanagement om de respons en paraatheid op incidenten te testen:

Dat kan van klein naar groot, in de volgorde

1. Technisch,
2. Theoretisch
3. Procesketen

Betrek de juiste mensen, bijvoorbeeld: SME, Senior proces operator, Productiehoofden, Proces automation engineer, of vergelijkbare rollen. Het gaat erom dat de betrokkenen in de oefening het proces en de productiedetails overzien. Belangrijk is dat alle betrokkenen praktijkkennis hebben van techniek en proces.

Dat kan van procedureel naar praktisch/operationeel:

- **Noodprocedures:** laat teams regelmatig oefenen op test- en noodprocedures met simulaties en zorg ervoor dat iedereen weet wat te doen in het geval van een incident en het personeel klaar is om effectief te reageren op veiligheidsincidenten. Na noodprocedure inbedrijfstelling van asset uitvoeren.
- **Tabletopoefeningen:** een scenario-gebaseerde discussie waarbij teamleden samenkomen om hypothetische situaties door te nemen. Dit is nuttig voor het testen van het besluitvormingsproces en het bespreken van strategieën zonder echte operationele verstoringen te veroorzaken. Dit helpt medewerkers om de implicaties van IACS-beveiligingsincidenten te begrijpen en hoe ze daarop moeten reageren.
- **Simulatie-oefeningen:** realistischere oefeningen waarbij een crisis wordt nagebootst om de reactietijd en effectiviteit van crisismanagementplannen in een gecontroleerde omgeving te testen.
- **Full-scale-oefeningen:** uitgebreide, grootschalige oefeningen waarbij alle aspecten van het continuïteits- en crisismanagementplan worden getest in een realistische setting en waarbij meerdere afdelingen betrokken zijn. Oefeningen die samenwerking tussen verschillende afdelingen vereisen, zoals IT, OT, en noodbeheer, helpen om een gecoördineerde crisisrespons te bevorderen. Dit kan worden gebruikt om zowel operationele als communicatiestrategieën te testen. Dit kunnen realistische scenario's zijn waarbij medewerkers hun respons op een IACS-incident moeten coördineren.

Oefeningen helpen om het vertrouwen van het team te vergroten in hun vermogen om een crisis effectief te beheersen Ze helpen bij het identificeren van hiaten of zwakke punten in de huidige plannen, wat cruciaal is voor voortdurende verbetering. Oefeningen verbeteren de samenwerking tussen verschillende afdelingen en teams binnen de organisatie.

Na elke oefening en ook na echte incidenten moet een gedetailleerde verslaglegging en evaluatie plaatsvinden, waarbij de prestaties van het team worden geanalyseerd en eventuele tekortkomingen worden gedocumenteerd en eventuele leermomenten te identificeren. De bevindingen van de oefeningen worden gebruikt om continuïteits- en crisismanagementplannen bij te werken, te verbeteren en te updaten. Het uitvoeren van een after action review na simulaties en echte incidenten is een manier om te bespreken wat er is geleerd en welke aanpassingen moeten worden gedaan.

Er zijn nog aanvullende manieren om te evalueren en verbeteren. Vraag regelmatig om feedback van medewerkers over de effectiviteit van de trainingsprogramma's en bewustwordingsinitiatieven. Gebruik deze feedback om verbeteringen door te voeren. Gebruik incidenten (zelfs kleine) als leermomenten om de bewustwording te vergroten. Bespreek wat er is gebeurd, wat goed ging en wat verbeterd kan worden. Indien mogelijk kunnen ook (regelmatige) beoordelingen en enquêtes uitgevoerd worden om het niveau van bewustwording binnen de organisatie te meten en te identificeren waar extra aandacht nodig is. Voer regelmatig veiligheidsbeoordelingen en audits uit om de effectiviteit van bestaande veiligheidsmaatregelen te evalueren en deze waar nodig aan te passen of te verbeteren.

Crisismanagementplannen worden bijgesteld op basis van evaluaties, nieuwe bedreigingsinformatie, technologische ontwikkelingen en veranderende bedrijfsbehoeften. Houd het plan up-to-date en pas het aan op basis van nieuwe evaluaties en veranderende bedrijfsbehoeften. Stel mechanismen in voor voortdurende monitoring en evaluatie van de geïmplementeerde maatregelen. Zorg ervoor dat de beveiligingsmaatregelen effectief zijn en voldoen aan het veranderende dreigingslandschap.

Bijlage 4: HSE

HSE (Health, Safety, and Environment) is binnen Operational Technology van groot belang in crisismanagement om verschillende redenen:

- **Veiligheid van werknemers:** tijdens een crisis, zoals een ongeval of een technische storing, is de veiligheid van de medewerkers van het grootste belang. HSE-voorschriften helpen bij het waarborgen van een veilige werkomgeving, wat cruciaal is voor het voorkomen van blessures en ongelukken.
- **Milieu-impact:** in veel sectoren kan een crisis leiden tot milieuvervuiling of andere negatieve milieueffecten. HSE-principes richten zich op het minimaliseren van deze risico's en zorgen ervoor dat maatregelen worden genomen om milieuschade te voorkomen.
- **Risicobeheer:** HSE-praktijken helpen bij het identificeren en analyseren van potentiële risico's, waardoor organisaties beter voorbereid zijn op crises. Dit omvat het opstellen van noodplannen en situatiesimulaties, zodat het personeel weet hoe te reageren.
- **Compliance en regelgeving:** organisaties moeten voldoen aan nationale en internationale HSE-regelgevingen. Niet-naleving kan leiden tot juridische problemen, boetes en reputatieschade, vooral in tijden van crisis.
- **Communicatie:** effectieve HSE-praktijken omvatten ook duidelijke communicatiekanalen en protocollen. In een crisis is het essentieel dat informatie snel en nauwkeurig wordt verstrekt aan alle betrokken partijen, inclusief medewerkers, autoriteiten en het publiek.
- **Herstel en continuïteit:** HSE is cruciaal voor het herstel na een crisis. Het helpt organisaties om terug te keren naar normale bedrijfsvoering en zorgt ervoor dat lessen uit de crisis worden geleerd om toekomstige incidenten te voorkomen.

Kortom, HSE speelt een integrale rol in het waarborgen van de veiligheid, gezondheid en milieu-invloeden in OT -Operational Technology, vooral binnen de context van crisismanagement.

IACS Coalitie

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.iacscoalitie.nl
Info@iacscoalitie.nl
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

september 2025