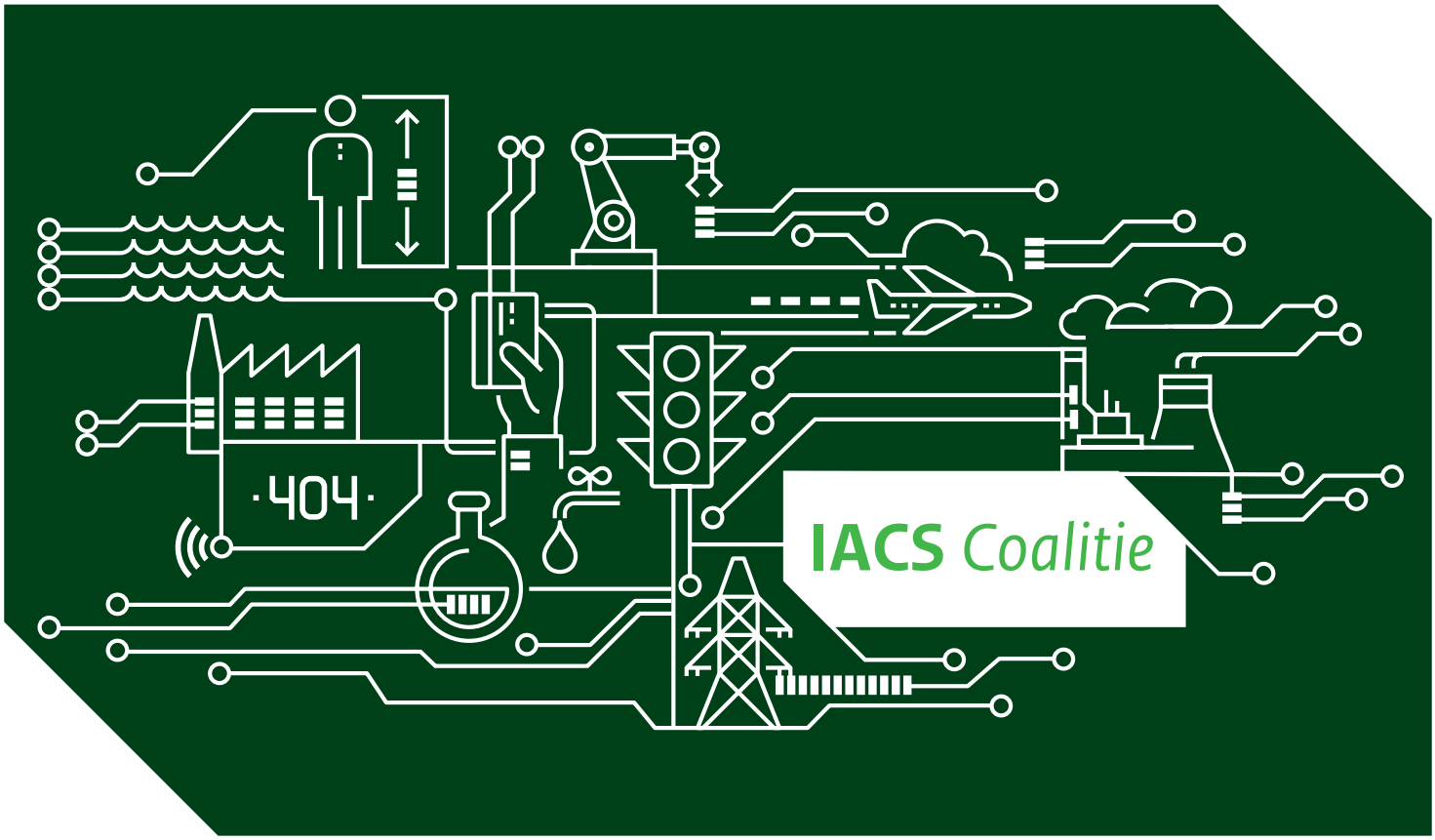

IACS Coalitie. Weerbaar. Samen.

Industrial Automation and Control Systems, ofwel IACS is een onmerkbaar, maar invloedrijk, onderdeel van het dagelijks leven. IACS wordt bijvoorbeeld in fabrieken toegepast om complexe processen soepel en effectief te laten verlopen, stuurt de verkeerslichten aan, zorgt dat de lift op de juiste verdieping stopt, regelt schoon drinkwater en beheerst dat het waterpeil in Nederland op het juiste niveau is.

De digitalisering van fysieke processen middels IACS brengt niet alleen vele voordelen met zich mee maar introduceert ook risico's van digitale dreigingen. Als een dergelijke dreiging zich voordoet in deze vitale processen, dan is er kans op (grote) schade aan mens en omgeving. Het is dus belangrijk om IACS digitaal weerbaar in te zetten. Deze ambitie wordt onderschreven door onder andere de Nederlandse Cyber-securitystrategie (NLCS) en implementatie van Europese richtlijnen als de Wet Beveiliging Netwerk- en Informatie-systemen (Wbni). De IACS coalitie heeft tot doel om deze ambitie te ondersteunen door samenwerking te versterken om zo effectief en efficiënt deze uitdaging samen aan te gaan.

Doelstelling IACS Coalitie

Bij veel organisaties zijn IACS ingezet en de aandacht hiervoor groeit, met name ook gericht op het verhogen van de digitale weerbaarheid. Er zijn grote verschillen te zien bij de diverse organisaties. De ene organisatie is al erg ver, terwijl de andere zich alleen nog maar net bewust is dat men er iets mee moet.

Het doel van de IACS Coalitie is om de ontwikkelingen en activiteiten op dit vakgebied te volgen, te bundelen, er richting aan te geven en de kennis hierover vanuit het collectief te delen met anderen. Door de samenwerking van diverse overheids-organisaties is dit collectief een krachtig orgaan voor zowel publieke als private organisaties om de digitale weerbaarheid van het IACS landschap te verhogen. Dit draagt daarmee direct bij aan een veiligere leefomgeving binnen Nederland.

Digitale weerbaarheid

Digitale weerbaarheid is het vermogen van IACS om cyberaanvallen te weerstaan, te detecteren en erop te reageren *(resilience)*.
Dit houdt in dat OT-systemen robuust en betrouwbaar moeten zijn en in staat moeten zijn om zichzelf te beschermen tegen bedreigingen en kwetsbaarheden. Het opbouwen van weerbaar-heid in OT-systemen is cruciaal om te voorkomen dat cyber-aanvallen leiden tot storingen in de vitale infrastructuur en om de continuïteit van de bedrijfsvoering te waarborgen.

Om de digitale weerbaarheid van OT-systemen te verbeteren, moeten belanghebbenden in de OT-sector samenwerken om een veilige en beveiligde omgeving te creëren. Door de digitale weerbaarheid van OT-systemen te verbeteren, kunnen belang-hebbenden in de OT-sector ervoor zorgen dat deze systemen veiliger en betrouw-baarder zijn en minder vatbaar voor cyber-aanvallen. Dit draagt bij aan de bescherming van de vitale infrastructuur en de veiligheid van de samenleving als geheel.

IACS Coalitie thema's

Awareness, Opleidingen, Trainingen en Oefenen
Creëren van bewustzijn, vergroten van kennis en vaardigheden van medewerkers in een noodsituatie door het bieden van (input op) communicatiemiddelen, trainingen en oefeningen.

Risicomanagement
Het gezamenlijk creëren van handreiking(en), tools en andere producten of diensten waarmee organisaties ondersteund worden in het beheer van hun risicomanagement.

Monitoring, Detectie en Respons
Middels een multidisciplinair team IACS monitoring, detectie en response door-ontwikkelen om organisaties hierop actief te houden. Daarnaast organisaties stimuleren om monitoring, detectie en respons toe te passen.
Bijvoorbeeld: een effectieve strategie of tool ontwikkelen om IACS te monitoren en bedreigingen te detecteren.

Onderzoek
Samenwerking tussen verschillende partijen om gevarieerde kennis en expertise te benutten voor het identificeren van onderzoekthema's, opzetten van onderzoekplannen/programma's, uitvoeren van onderzoek en het delen en presenteren van bevindingen en aanbevelingen aan belanghebbenden. De output van de onderzoeken kunnen tevens als input gebruikt worden voor de andere thema's.

Business Continuity Management, Crisis management en de CERT functie
Gezamenlijk stimuleren om de continuïteit van de organisatie te borgen middels een geactualiseerde integrale aanpak.
Bijvoorbeeld: ontwikkelen van een uitgebreid plan voor IACS verstoringen voor verschillende sectoren.

Samen

Omdat IACS vaak complex en en veelal onderling verbonden is samenwerking bij de bescherming van OT van cruciaal belang. Ten eerste zijn er veel verschillende belanghebbenden betrokken bij de bescherming van OT-systemen, waaronder regelgevers, exploitanten van kritieke infrastructuur, technologieproviders, beveiligingsbedrijven en meer. Effectieve samenwerking tussen hen is essentieel om de veerkracht en bescherming van deze systemen te waarborgen.

Het delen van informatie over bedreigingen en kwetsbaarheden tussen deze belanghebbenden, het ontwikkelen van gemeenschappelijke beveiligingsstandaarden en -protocollen, en het opzetten van gemeenschappelijke trainingsprogramma's voor beveiligingspersoneel is nodig om OT goed te kunnen beschermen. Daarnaast helpt samenwerking om efficiënter en effectiever om te gaan met de schaars beschikbare kennis op IACS gebied. Cyberdreigingen evolueren voortdurend en worden steeds complexer. Om deze dreigingen effectief te kunnen aanpakken, is het noodzakelijk om voortdurend samen te werken en samen te leren van nieuwe bedreigingen en aanvalstechnieken. Door samen te werken kunnen belanghebbenden in de OT-sector ervoor zorgen dat de beveiliging van deze vitale systemen voortdurend wordt verbeterd en aangepast aan de veranderende bedreigingsomgeving.

IACS Coalitie is een samenwerking tussen het Ministerie van Infrastructuur en Waterstaat, Nationaal Cyber Security Center, Rijksinspectie Digitale Infrastructuur en de Informatiebeveiligingsdienst.