Recommendation on the digital security of Industrial Automation & Control Systems (IACS) in the critical national infrastructure of the Netherlands

CSR
Cyber Security Council
Cyber Security Raad

Recommendation on the digital security of Industrial Automation & Control Systems (IACS) in the critical national infrastructure of the Netherlands

Cyber Security Council Cyber Security Raad

Addressed to:

The Minister of Justice and Security
The State Secretary for Economic Affairs and Climate Policy
The Minister of the Interior and Kingdom Relations
Other ministers and state secretaries whose providers of critical services are subject to the Directive on security of network and information systems (NIS Directive)
The competent authorities

24 April 2020

CSR Recommendation 2020, No. 2

Your Excellency,

We hereby present the recommendation of the Cyber Security Council (hereafter: the CSR) regarding the digital security of Industrial Automation & Control Systems (IACS)[1] in the critical national infrastructure of the Netherlands.

Protecting what is ours

The digitalisation of production processes will continue to increase over the coming years, which in turn will increase our society's dependence on ICT and IACS. Effective protection of critical production and ICT processes is therefore crucial. The majority of IACS are ICT-based measurement and regulation systems that are used to manage our production processes. IACS are therefore critically important to preserving the continuity of the country's critical national infrastructure, as interference with this infrastructure may cause major social disruption and erode public trust in digitalisation. Such interference can result in the failure of systems and objects that allow our society and economy to function. IACS make it possible for our locks and bridges to function, for electric power and gas to be distributed, for drinking water to be purified and for nuclear waste to be processed. They ensure that trains arrive at their destination, containers are transported and lifts are able to operate. The ongoing coronavirus crisis underscores the urgent nature of cybersecurity in relation to IACS: critical services must be able to function at all times.

We must devote continuous attention to maintaining and/or improving the IACS that support critical processes. At the same time, it is important to note that non-critical processes are interwoven with critical national infrastructure, and that IACS are often indirectly connected to the Internet, which means that a disruption, whether intentional or not, may have consequences across the entire chain. We would therefore do well to focus on critical sectors, as well as on critical providers. Studies conducted by the Netherlands Scientific Council for Government Policy (WRR)[2] and the Netherlands Organisation for Applied Scientific Research (TNO)[3] draw attention to the risks that new and existing chain dependencies pose to IACS at the sector and cross-sectoral level. It is also important to keep the international aspect in mind. The interdependencies of many critical processes – energy being one example – do not end at the national border. Cascade effects may occur either within a single country or back and forth between multiple nations. The Netherlands must be prepared to counter this risk as well.

Because IACS play a crucial role in protecting our critical national infrastructures, they deserve our attention on a permanent basis. In addition, the increasing use of generic ICT tools in IACS is introducing the standard ICT problems into industrial automation. Exploitation of the vulnerabilities in IACS could lead to severe economic losses and social disruption. Despite this, the majority of efforts in the Netherlands are aimed at enhancing the cybersecurity of ICT. So far, like many other countries, the Netherlands has not yet experienced severe consequences as a result of an IACS-related cyber incident involving the critical national infrastructure. This does not mean it is safe for us to relax and assume the worst will not happen here. There are a number of examples of disruptive IACS failure, though

[1] In 2019, for the purposes of this recommendation, the CSR commissioned research company Gartner to conduct a preliminary inquiry.

[2] Netherlands Scientific Council for Government Policy (2019), *Voorbereiden op digitale ontwrichting* [Preparing for digital disruption], WRR Report 101, The Hague

[3] Advisory report *'Intersectorale afhankelijkheden: buitenlandse methoden en mogelijke toepasbaarheid in Nederland*' [Cross-sectoral Dependencies: Foreign Methods and Their Potential Applicability in the Netherlands] (2013), TNO, commissioned by the then Ministry of Security and Justice and the Research and Documentation Centre (WODC)

these have taken place outside of the critical national infrastructure in the Netherlands (NotPetya[4]) and in regions other than Western Europe (BlackEnergy[5] and Stuxnet[6]). Closer to home, NotPetya has caused considerable harm in the United Kingdom.

The increasing connectivity of IACS,[7] in combination with outdated legacy systems, renders the critical national infrastructure vulnerable both to accidental failure and malicious actors. It is therefore reasonable to assume that coordinated, simultaneous attacks on the critical national infrastructure could take place in the future. In the Netherlands, the General Intelligence and Security Service (AIVD) warns that state actors are attempting to gain access to our critical processes.[8]

It is important to protect what is ours. We must preserve our ability to take decisive action in response to wrongdoing and/or cyberattacks.

We have not always structured our affairs as effectively as we should

We need to be aware that the threat environment is continuously shifting. New threats and chain dependencies may increase the vulnerability of certain objects, necessitating different or additional measures. This, in turn, makes it necessary to allocate different or extra resources and people to align the necessary measures with the identified risks – which is why digital resilience is a boardroom issue. IACS-related studies conducted by various institutions show that, in practice, this is not always sufficiently the case. A study by the Netherlands Court of Audit,[9] for instance, found that efforts to ensure the digital resilience of our flood defences are currently not going to plan, despite the Dutch government's leading and exemplary role in this area. The Directive on security of network and information systems (NIS Directive) sets out the legislative tasks of the ministries[10] involved and defines the competent authorities[11] for all critical sectors. Under the NIS Directive, responsibility for managing risks associated with external dependencies on third parties lies with the individual provider of the essential service in question. As a result, there is limited insight into the risks and dependencies that exist between government and businesses in the various critical sectors.

In other words, since no complete picture of the threats and risks in our critical sectors is available to us, we do not know whether we can protect ourselves effectively.

Furthermore, it appears we are insufficiently prepared to deal with the consequences of IACS failure. The Cyber Security Assessment Netherlands (CSAN) 2019[12] and the WRR advisory report 'Preparing for

[4] Variants of Petya were first detected in March 2016. They spread via files sent as email attachments. In June 2017, a new Petya variant called NotPetya was deployed in a worldwide cyberattack, the primary target of which was Ukraine.
[5] BlackEnergy malware was used in attacks on power plants in 2016. As a result of the attacks, some 700,000 people in Ukraine found themselves without electricity for several hours.
[6] Stuxnet is advanced malware first discovered by a Belarusian manufacturer of antivirus software in June 2010. The program has a detrimental effect on the operation of certain Siemens appliances.
[7] Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands (2019), University of Twente, commissioned by the Research and Documentation Centre (WODC)
[8] 2018 AIVD Annual Report, General Intelligence and Security Service, 2019
[9] *Digitale dijkverzwaring: cybersecurity en vitale waterwerken* [Strengthening the digital defences: the cyber security and critical water structures] (2019), Netherlands Court of Audit.
[10] This involves the Ministry of Justice and Security and the Ministry of Economic Affairs and Climate Policy.
[11] Section 4.1 of the Network and Information Systems Security Act (Wbni) defines the following as competent authorities: the Ministry of Economic Affairs and Climate Policy (Radiocommunications Agency Netherlands), the Ministry of Finance (De Nederlandsche Bank N.V.), the Ministry of Infrastructure and Water Management (Human Environment and Transport Inspectorate) and the Ministry of Health, Welfare and Sport (Health and Youth Care Inspectorate).
[12] Cyber Security Assessment Netherlands (CSAN) 2019, National Coordinator for Security and Counterterrorism (NCTV), 2019

digital disruption'[13] show that the Netherlands is insufficiently prepared to deal with potential digital disruption and to deliver the legally enshrined support that will be needed should this risk materialise. The CSR considers this situation to be undesirable and is of the opinion that:

Dutch society must be able to rely on the security and continuity of the country's critical national infrastructure. The digital resilience of the critical providers' IACS must be brought up to the required standard, to a level that is appropriate and proportional in light of the threats and risks.

[13] Netherlands Scientific Council for Government Policy (2019) *Voorbereiden op digitale ontwrichting* [Preparing for digital disruption], WRR Report 101, The Hague

RECOMMENDATIONS

The Dutch government recognises the necessity of effective supervision of digital security to ensure continuous efforts towards a high level of digital resilience and continuity. The critical sectors differ from one another in terms of the maturity of their digital resilience. The CSR commissioned research company Gartner to conduct a study into the nature and scope of IACS-related problems. The main recommendations resulting from that study are that the IACS administrators[14] have a need for greater chain-oriented coordination between the critical sectors, better information exchange, and support in certain areas with regard to purchasing IACS. The Netherlands Organisation for Applied Scientific Research echoes these findings in its study on success factors for digitally secure IACS.[15]

In conjunction with one another, the following three measures ensure greater insight, supervision and robustness of the IACS and therefore serve to enhance the digital resilience of the Netherlands:

1. **Without exception, every critical sector must have an individual sectoral IACS control framework in place. Supervision will be proportionally strengthened where needed.**
2. **IACS-related knowledge will be bundled and the exchange of classified information regarding IACS threats will be more effectively facilitated.**
3. **IACS administrators will be more effectively supported in their procurement processes.**

Re 1. Without exception, every critical sector must have an individual sectoral IACS control framework in place. Supervision will be proportionally strengthened where needed.

The great importance of continuity for critical providers, in combination with the increase of digital threats, calls for a structural focus on digital resilience. In its policy response to the CSAN 2019, the Dutch government indicates that the security of critical sectors must be safeguarded. Likewise, IACS administrators must maintain continuous awareness of the state of affairs regarding the digital resilience of their organisations. They have indicated that there is a need for a clear and broadly supported framework of cybersecurity measures.[16] This framework should establish what will be expected of the organisations in order to preserve the digital resilience of their IACS. Given the nature and complexity of the issues at hand, coordination in drafting the framework between sectoral supervisory authorities, administrators and IACS suppliers will be both necessary and the key to success.

[14] IACS administrators are all organisations responsible for the management of IACS in connection with critical processes. This includes both critical providers and the companies to whom portions of critical processes have been outsourced.
[15] Advisory report '*Succesfactoren voor digitaal veilige Operationele Technologie*' [Success factors for digitally secure Operational Technology] (2019), TNO
[16] This is one of the conclusions of the preliminary inquiry conducted by Garner in 2019 at the behest of the CSR.

Standardisation, certification and harmonisation – in the sectors and in the market – should be the central priorities of these frameworks. Today, these crucial matters are recognised and are being addressed at the European level as well. The Cybersecurity Act[17] will play an important role in these efforts. It is possible to involve supervisory authorities in the process by which the market, policymakers and implementing bodies are developing these frameworks. Jointly drafting a sector-specific IACS control framework will enhance uniformity and create a broader base of support while taking sector-specific working methods into account. The CSR recommends that the sectoral IACS control frameworks should be coordinated with ongoing European initiatives.

The framework may also assist less 'mature' IACS administrators in their efforts to enhance the digital security of their systems. A number of critical sectors in the Netherlands, including nuclear power and water supply, have already developed their own sectoral control frameworks independently. Their knowledge and experience offer a basis for developing an approach that all critical sectors can use to draft IACS control frameworks for themselves. Above all, we must work together to make use of what is already available.

The CSR bases its recommendation in part on the approaches in the United Kingdom and Germany, where sectoral control frameworks for critical sectors have already proven successful. Based on those experiences, it would be advisable to have the sectoral IACS control frameworks evaluated by an independent third party in the future.

The CSR recommends that the competent authorities, in cooperation with the sector supervisory bodies and the IACS administrators, ensure the implementation of sectoral IACS control frameworks in all critical sectors.

Enhancing the supervision of digital resilience

The CSR advocates an active approach to supervision within the statutory frameworks (Wbni). It is important that all parties have a clear understanding of how this supervision is arranged and what the consequences will be should they break the rules. Supervisory authorities can take the IACS control frameworks as a starting point for their supervision and then reflect back on them to achieve a continuous improvement cycle and ensure that responsibility remains where it should, with the companies and institutions themselves. Based on the respective sectoral IACS frameworks, supervision can then be proportionally strengthened where necessary.

The CSR considers it crucial that all critical sectors have a sectoral IACS control framework in place within two years from now, that they report on this framework to the designated competent authorities. These authorities must be able to evaluate the results based on these frameworks.

Re 2. IACS-related knowledge will be bundled and the exchange of classified information regarding IACS threats will be more effectively facilitated.

It is a source of concern to the CSR that the exchange of knowledge and information regarding the digital resilience of our society remains problematic. In 2017, the CSR called for extensive attention to this issue and recommended the establishment of a nationwide network of information exchanges to ensure that all businesses and organisations in the Netherlands will have ready access to information

[17] The EU Cybersecurity Act: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

on cybersecurity.[18] This year, the National Coordinator for Security and Counterterrorism[19] and the WRR[20] have noted that the current information provision has still not reached the required level. As it stands now, the information exchange is somewhat discretionary in nature, as providing relevant information is not always mandatory or may be impossible under the prevailing laws and regulations. Parties are often hesitant to share information when they are not obligated by law to do so. Furthermore, the exchange of specific information is sensitive due to competition issues, legal restrictions, national security and the dual role of the government, which may use the information obtained for the purpose of audits. The inadequate exchange of information is even more apparent with regard to information on IACS.

Bundling the scarce IACS expertise available

The development of knowledge regarding IACS is necessary to guarantee that the critical providers have sufficient digital resilience, and therefore to ensure the continuity and integrity of the systems. Information Technology (IT) and Operational Technology (OT) specialists cannot afford to operate in separate spheres. The strengths of these two domains – which for the most part have operated independently of one another until now – must be bundled.

All stakeholders involved, including the National Cyber Security Centre (NCSC), the sectoral supervisory authorities and the IACS administrators in the critical sectors, must therefore have the knowledge required to discuss these issues with one another and with other countries. In various other nations, employees at supervisory bodies and in the specialised IACS-focused departments of their NCSCs have obtained individual knowledge of critical sectors through sector-specific training and education programmes. The CSR believes that the Netherlands must follow this example. Sectoral supervisory bodies, including Radiocommunications Agency Netherlands and the NCSC, must include a sufficient number of experts to ensure they are able (within the bounds of their statutory tasks and responsibilities) to contribute to the digital resilience of IACS in the critical sectors. Since IACS-related knowledge has proven scarce in practice, it is vital to make maximum use of the existing expertise. Public and private organisations can strengthen one another's efforts in this regard. To that end, a formal public-private network of experts must be established under the coordinating leadership of the NCSC. IACS providers must be part of this network whenever possible as well. It is vital that experts have ready access to other experts, even those outside their respective sectors. With that in mind, it would be prudent to further optimise the Information Sharing & Analysis Centres (ISACs) along these cross-sectoral lines and to continue to promote knowledge exchange in connection with ISACs.

Establishing trusted channels between the government and critical national infrastructure

In addition to knowledge sharing, the exchange of intelligence on IACS-related threats is crucial as well. Sharing information regarding these threats is an especially delicate matter, as state actors may be involved and the failure of IACS may result in social disruption and considerable liability. One obstacle to information exchange is the fact that highly classified threat intelligence may be shared only under strictly defined conditions. Such intelligence can only be transmitted if mutual trust exists between the providers and administrators of IACS, and if governmental bodies such as the NCSC and the intelligence agencies share such information as well. The CSR therefore recommends – in addition to the regular method of sharing information within the nationwide network of information exchanges

[18] CSR Recommendation 2017, No. 2: '*Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime*' [Towards a nationwide system of information exchanges, advice on information sharing with regard to cyber security and cybercrime]

[19] Cyber Security Assessment Netherlands (CSAN) 2019, National Coordinator for Security and Counterterrorism (NCTV), 2019

[20] Netherlands Scientific Council for Government Policy (2019) *Voorbereiden op digitale ontwrichting* [Preparing for digital disruption], WRR Report 101, The Hague

– that trusted channels be created for the purpose of sharing classified information (on threats, etc.) between all government bodies (NCTV, AIVD/MIVD, NCSC and supervisory authorities) and individual administrators within the critical sectors. One instrument for achieving this is the appointment of a Security Liaison Officer (SLO). The SLO acts as a confidential adviser within an organisation that uses IACS as part of a critical process; the SLO has been subject to security screening[21] as set out in the Security Screening Act (Wvo).

Setting up regular cyber exercises

Bundling scarce knowledge and improving the provision of information are preconditions for enhancing digital resilience among IACS administrators. Another important contributing factor for a more robust digital resilience is a regular schedule of joint cyber exercises, including cross-border exercises. More sector-specific exercises must be developed and conducted for IACS; these will need to include attention to cross-sectoral and international dependencies. Practice makes perfect and this applies to digital resilience as well.

Re 3. IACS administrators will be more effectively supported in their procurement processes.

In the critical sectors, the procurement of IACS only takes up a small part of the budget for any given infrastructure project. As a result, a party that specialises in that physical component will often subcontract a different party for the IACS. If we are to safeguard continuity and integrity, parties on both the supply and the demand sides of the equation must approach IACS as a critical component for which digital resilience must be contractually assured. To that end, the CSR believes that organisations require support in a number of areas: the development of model contract clauses, the exchange of information regarding vulnerabilities in IACS and the ability to exclude specific providers under certain conditions. The study conducted by Gartner confirmed this. Administrators have indicated the need for government support when negotiating appropriate cybersecurity agreements with their providers during the procurement process and when using the systems. Cybersecurity-related terms and conditions must become a standard part of contractual provisions, e.g. pertaining to the security of design principles and the degree to which providers will update their products, as well as terms regarding the reliability of the providers themselves. In light of the international nature of most providers, certification should ideally take place at the European level. This is in keeping with the ambition of the Dutch National Cyber Security Agenda (NCSA)[22] and the Roadmap for Digital Hard- and Software Security[23], in which the Dutch government expresses its desire to promote standards and certification that will be widely accepted (across Europe and even globally) and will serve to enhance digital resilience. The EU Cybersecurity Act[24], which recently entered into force, contributes to this as well.

Exclusion of specific providers

In its recommendation regarding 5G[25], the General Intelligence and Security Service (AIVD) confirmed the risk posed by implantation in the Dutch critical national infrastructure for the purpose of potential

[21] This functionality already exists in several EU countries and has been laid out in the European Programme for Critical Infrastructure Protection (EPCIP) directive.
[22] National Cyber Security Agenda: A cyber secure Netherlands, National Coordinator for Security and Counterterrorism (NCTV), on behalf of the Dutch government, 2018
[23] Roadmap for Digital Hard- and Software Security, Ministry of Economic Affairs and Climate Policy and Ministry of Justice and Security, 2018
[24] The EU Cybersecurity Act: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[25] *Advies Nationale Veiligheid en Veiling 5G* [Recommendation on national security and 5G auction], General Intelligence and Security Service of the Netherlands, 2019

sabotage. Based on objective criteria, the recommendation by the AIVD offers IACS administrators the possibility to exclude specific telecom providers from the procurement process. A previous precautionary measure introduced by the government in connection with Kaspersky antivirus software (which alerted companies involved in critical national infrastructure to the government's reasons for discontinuing the use of this software) exposed the necessity of establishing objective criteria[26] as a means of making it legally possible to exclude suppliers from tenders. The CSR therefore advises conducting similar risk analyses within critical processes in order to provide these IACS administrators with the legal tools (set out by the government) needed to exclude certain providers from participating in tenders for sector-specific subprocesses.

Establishment of an IACS Support Centre

The CSR believes that the aforementioned support must be transparent and readily accessible to IACS administrators. The CSR recommends that the NCSC establish an IACS Support Centre, either physical or virtual, in cooperation with the other supervisory authorities and relevant parties. One objective of this Support Centre is to assist IACS administrators in their procurement processes by providing relevant cybersecurity-related knowledge and compiling and sharing reports of vulnerabilities among providers and administrators. In Germany, agreements between the government and IACS suppliers have been formally set out in a Charter of Trust. The Support Centre should follow this example, and should additionally identify any legal obstacles to sharing information regarding IACS. All relevant cybersecurity information must be shared in order to provide the IACS administrators (including those who are not yet fully informed) with a proper basis for determining a course of action. This will allow IACS providers to distinguish themselves from competitors and will enhance confidence in these systems.

[26] The following criteria have been adopted in the Resolution on Telecommunications Security and Integrity:
a. a state, entity or natural person that is known or can be suspected to have the intention to abuse or cause disruption of an electronic communications network or service being provided in the Netherlands, or;
b. maintains close ties or is under the influence of a state, entity or natural person as referred to in a., or an entity or person that can be suspected to maintain such ties or be subject to such influence.

TARGETED RECOMMENDATIONS

These recommendations are aimed at the government and, through the government, the business community. Only through improved coordination between the public and private sectors can the digital resilience of IACS in critical processes be strengthened and will Dutch society be able to rely on the security and continuity of the country's critical national infrastructure. To that end, the CSR recommends the following:

Ministers and state secretaries whose providers of critical services are subject to the Directive on security of network and information systems (NIS Directive):

1. should, within two years' time, ensure that each critical sector has a sectoral IACS control framework in place and reports on this framework to the supervisory authorities;
2. should explore the possibility of having the sectoral control frameworks evaluated by an independent third party.

The Minister of Justice and Security and the State Secretary for Economic Affairs and Climate Policy, in joint action:

3. should, within one year's time, establish an IACS Support Centre, either physical or virtual, where IACS suppliers and administrators in critical sectors can report IACS-specific vulnerabilities and receive advice on digital resilience in connection with the procurement and replacement of these systems.

The Minister of Justice and Security:

4. should ensure that, within two years' time, sufficient sector-specific expertise regarding IACS is developed within the National Cyber Security Centre (NCSC);
5. should, within two years' time, establish a formal public-private network of IACS experts, promote the attainment of an equal maturity level among Information Sharing & Analysis Centres (ISACs) and stimulate their continued cross-sectoral development;
6. should, every two years, arrange for parties in the critical national infrastructure to conduct at least one IACS-oriented exercise (each aimed at a single, specific critical process); should, at least once every four years, include cross-sectoral and international dependencies in these exercises as well.

The Minister of Justice and Security and the Minister of the Interior and Kingdom Relations, in joint action:

7. should, in cooperation with the critical sectors, realise trusted channels within one year's time.

All competent authorities:

8. should proportionally strengthen supervision where necessary, based on the sectoral control frameworks;

9. should, within two years' time, have supervisory authorities with sufficient sector-specific specialist expertise regarding IACS.

The Hague,

On behalf of the Cyber Security Council,

Hans de Jong
CSR co-chair

Pieter-Jaap Aalbersberg
CSR co-chair