Good practice guide for CERTs in the area of Industrial Control Systems

Computer Emergency Response Capabilities considerations for ICS

October 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Andrea Dufkova (ENISA)

Joshua Budd, Jachym Homola and Matthew Marden (IDC CEMA)

Contact

For contacting the authors please use cert-relations@enisa.europa.eu

For media enquiries about this document please use press@enisa.europa.eu.

Acknowledgements

We would like to thank all the CERTs and other organisations that participated in the survey or the interview conducted for the purpose of this document.

Terminology

The term CERC (Computer Emergency Response Capabilities) or ICS-CERC (Industry Control Systems CERC) will be used throughout this document to depict the capabilities that a Computer Emergency Response Team (CERT) needs to develop in order to provide services for the protection of ICS and ICS networks. For better readability by avoiding repetition of abbreviations a couple of synonyms will be used, depending on the context (i.e. 'ICS-CERC services' to depict those services, 'ICS responsibility' to point to the overall mandate of a CERT in that context, etc.).

Executive summary

Industrial **C**ontrol **S**ystems (ICS) are indispensable for a number of industrial processes, including energy distribution, water treatment, transportation, chemical, government, defence and food processes. Though until a few decades ago ICS functioned in discrete environments, nowadays they tend to be connected to the Internet. This enables streamlining and automation of industrial processes, but carries with it the risk of exposure to cyber-attacks. The ICS are lucrative targets for intruders like criminal groups, foreign intelligence, phishers, spammers or terrorists. Therefore, the ability to respond to and mitigate the impact of ICS incidents is crucial for protecting critical information infrastructure and enhancing cyber-security on a national, European and global level.

This document is an initial attempt to provide a good practice guide for the entities that have been tasked to provide **ICS C**omputer **E**mergency **R**esponse **C**apabilities (ICS-CERC). On the other hand, this guide does not have the ambition to prescribe to the EU Member States which entities should be entrusted with provision of ICS-CERC services.

This document builds upon the current practice of CERTs with responsibilities for ICS networks, and also on the earlier work of ENISA on a baseline capabilities scheme for national/ governmental (n/g) CERTs[1]. Consequently, it employs a similar approach in addressing the topics relevant for ICS-CERC provision, by using four categories of baseline capabilities: mandate, service portfolio and operations in relation to ICS-CERC and, last but not least, cooperation with the other ICS stakeholders. These four categories of capabilities are mutually interdependent.

In the chapter on **mandate capabilities** the guide delves into formal processes for the establishment of ICS-CERC. It mentions factors that need to be taken into account when building ICS-CERC rather than building response capabilities for 'ordinary' ICT systems. The guide also addresses the advantages and disadvantages of concrete types of the mandate: ICS sector-specific, national, regional and global. It defines the constituencies for ICS-CERC and offers a variety of international sources of inspiration for the mandate and other formal aspects of ICS-CERC.

O**perational capabilities (technical)** focus on actual ICS-CERC services to be provided, especially in the main phases of the incident management cycle. The guide also briefly touches upon the question of how to maintain, develop and improve ICS-CERC once it has been established.

The chapter on **operational capabilities (organisational)** deals with operational aspects required for the provision of ICS-CERC services and also with dedicated personnel and their qualifications. The guide highlights the importance of training and further education for the staff responsible for ICS-CERC and also raises the topic of a suitable hosting organisation for ICS-CERC.

The chapter on **co-operational capabilities** summarises the main reasons for on-going cooperation between CERTs providing ICS-CERC services and other ICS stakeholders. In this context, the peculiarities of both national cooperation (with ICS providers, vendors or CERTs in the country) and

[1] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

cross-border cooperation (international initiatives in the area of ICS protection like CIGRE, ESCoRTS, IEEE and others) are discussed.

Wherever appropriate, examples of current practices related to handling ICS incidents are presented. However, it should be noted that established CERTs in Europe still have very limited experience in and contact with ICS-CERC services. For these reasons, this guide needs to be considered a living document, which will need to be updated in accordance with wider deployment of ICS-CERC in Europe. ENISA is ready to provide support to the teams responsible for the provision of ICS-CERC services. It already provides online training material for the CERTs relating to attacks on critical information infrastructure (scenario 13 of CERT training material[2]).

[2] http://www.enisa.europa.eu/activities/cert/support/exercise

Table of Contents

1 Introduction

1.1 Aim and scope of the document

The objective of this guide is to provide good practice to build a Computer Emergency Response Capabilities for Industrial Control Systems (ICS-CERC). It aims to support those teams that will be entrusted with the provision of ICS-CERC in the EU Member States, and for the governments that consider assigning a mandate for ICS-CERC to a team. The aim of the guide is not to make recommendations on which bodies should be responsible for the provision of ICS-CERC. Such a decision is within the competence of the EU Member States.

The guide builds on the current good practice of CERTs that are tasked with dealing with ICS security incidents and on earlier work of ENISA in defining baseline capabilities for n/g CERTs.[3] The four categories of baseline capabilities (mandate & strategy, services, operation, cooperation) defined previously by ENISA to describe a properly functioning CERT are, with some adjustments, the basis of this document. Section 2, the core of the guide, examines in detail the four categories of baseline capabilities required for the establishment and effective provision of ICS-CERC services.

Subject matter stakeholders were consulted. A number of CERTs in Europe and worldwide were asked to respond to a survey on aspects of the above-mentioned four baseline capabilities in the area of ICS protection. Several subsequent interviews were conducted with the representatives of the crucial stakeholders: CERTs, ICS asset owners and vendors. The main and most interesting ideas and opinions of these stakeholders are highlighted throughout the document.

1.2 European policy environment with regard to ICS-CERC and Critical Information Infrastructure

Industrial control systems often constitute Critical Information Infrastructures (CII).[4] The EU and its Member States are aware of the increased exposure of ICS to outside malicious attacks. At the European level the EU Member States are working on countermeasures to protect CII.[5] An important step was the adoption of the Directive on European Critical Infrastructures[6] in 2008. The Directive established a procedure for identifying and designating European Critical Infrastructures (ECI)[7] and a common approach for assessing the need to improve their protection. However; the Directive has a rather sectorial scope, and refers only to the energy and transport sectors. In 2012, the Directive

[3] ENISA, Baseline Capabilities for National/ Governmental CERTs (2009); Deployment of Baseline Capabilities of National / Governmental CERTs: Status Report, 2012.

[4] Critical information infrastructure was defined in a Green Paper on a European Programme for Critical Information Infrastructure Protection, COM (2005) 576 final, as 'including those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments'.

[5] https://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip

[6] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm

[7] Critical infrastructure was defined in a Green Paper on a European Programme for Critical Information Infrastructure Protection, COM(2005) 576 final, as 'including those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments'.

was comprehensively reviewed.[8] As a result, the scope of the Directive may be extended in the future to other sectors that rely heavily on CII and ICS.

There have been a number of initiatives by European institutions dealing with the topic of CII Protection (CIIP). In 2009 the European Commission adopted a **Communication on Critical Information Infrastructure protection (CIIP)**.[9] The Communication included an action plan for both the EU Member States governments and the private sector. It was based on five pillars: (i) preparedness and prevention, (ii) detection and response, (iii) mitigation and recovery, (iv) international cooperation and (v) criteria for European Critical Infrastructures in the field of ICT.

Two years later another communication was published on the results achieved in meeting the objectives of the action plan: **Communication on CIIP on 'Achievements and next steps: towards global cyber-security'**.[10] The European Commission took stock of the results achieved so far and announced follow-up actions. This Communication concluded that purely national approaches to tackling security and resilience challenges are not sufficient, and that Europe should continue its efforts to build a coherent and cooperative approach across the EU.

In its **Conclusions on CIIP**[11] of 27 May 2011, the Council of the European Union stressed, among other things, the need to foster cooperation among Member States by developing incident cooperation mechanisms between them. In addition two **ministerial conferences on CIIP** were held: in 2009 (Tallinn, Estonia)[12] and in 2011 (Balatonfüred, Hungary).[13] In Tallinn, the debate ('Tallinn process') started on the general direction of the European efforts towards an increased network and information security for CIIP. The conference in Balatonfüred aimed to take stock of progress made and lessons learned (reflected in the above-mentioned Council conclusions). It also discussed ways to engage all relevant stakeholders and in particular the private sector.

In 2012, the European Parliament adopted a **resolution** on the European Commission's **Communication on CIIP on 'Achievements and next steps: towards global cyber-security'**.[14] The resolution included recommendations that have subsequently been incorporated into the **EU Cyber Security Strategy** and into the accompanying proposal for a Directive on network and information security.[15] The EU Cyber Security Strategy explicitly mentions that the Commission and EU Member States will 'increase policy coordination and information sharing through the international Critical Information Infrastructure Protection networks such as the Meridian network,[16] cooperation among competent authorities for network and information security and others'.

[8] See a working document of the European Commission: http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF
[11] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede150611cccybersecurity_/sede150611cccybersecurity_en.pdf
[12] http://www.mkm.ee/eu-ministerial-conference-in-estonia-initialized-tallinn-process-to-secure-critical-information-infrastructure/
[13] http://www.newspusher.com/EN/post/1302809161-2/EN-/telecom-ministerial-conference-on-ciip-balatonfured.html
[14] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167
[15] http://www.eeas.europa.eu/policies/eu-cyber-security/
[16] http://www.meridian2007.org/Default.aspx

In this strategy the European Commission asks ENISA to:

- Assist the EU Member States in developing strong national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure;
- Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU (the task that lead to the development of this guide).[17]

The overall EU policy on CIIP has resulted in a number of concrete achievements. As a follow-up to the Communication on CIIP (see footnote 9), the European Forum for Member States and the **European Public-Private Partnership for Resilience**[18] were established. In addition, **two pan-European cyber exercises** (Cyber Europe 2010[19] and 2012[20]) **and one EU–US cyber exercise** (Cyber Atlantic in 2011[21]) have taken place. The objective of these exercises was to trigger communication and collaboration between EU Member States when responding to large-scale attacks affecting CII.

In 2010 ENISA published a minimum set of **baseline capabilities** and related policy recommendations **for National/ Governmental Computer Emergency Response Teams (CERTs**) to function effectively. In 2012, ENISA took stock of the progress made and updated policy recommendations.[22]

In recent years ENISA has researched several issues related to CIIP, with an emphasis on improving the protection and resilience of ICS. In December 2011, it published a report **'Protecting Industrial Control Systems: Recommendations for Europe and Member States**',[23] with extensive analysis of the ICS protection in Europe and beyond. It also includes ICS security standards and guidelines (Annex III) as well as a list of initiatives in ICS security (Annex IV).

EU Member States have also made progress in adopting national cyber-security and CIIP strategies. Usually, the national cyber-security strategy deals with CIIP issues,[24] while a separate strategy is less common. Germany is an example of a Member State that has both a 'general' cyber security strategy and a strategy on CIIP.[25]

[17] This task is in fact analogous to earlier work by ENISA in the area of baseline capabilities for n/g CERTs
[18] https://resilience.enisa.europa.eu/ep3r
[19] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report
[20] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1
[21] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic/cyber-atlantic-2011
[22] http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities
[23] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems
[24] ENISA maintains a selection of national cyber-security strategies at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.
[25] http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

2 Recognised practices for ICS-CERC

As ICSs become increasingly interconnected and thus more vulnerable to and a greater target of cyber-attacks,[26] it is also becoming more important that ICS computer emergency response capability (ICS-CERC) is in place to counter these threats. ICS-CERC can be developed and offered by many different entities, including CERTs, governmental organisations, non-governmental organisations and private corporations. Incident handling is a core ICS capability that must be provided by any such actor, but the specific nature of the ICS cyber-security arena means that teams with ICS-CERC will often also serve other functions such as sharing and distributing information about ICS cyber-security incidents or collecting statistics about ICS incidents.

The challenges in developing these capabilities have many similarities to those faced in the broader ICT environment, but also key differences can be observed.[27] ICS-CERC have to be built up with those differences in mind. Still, the overlap between the capabilities needed for responding to ICS cyber-incidents and ICT cyber-incidents means that the experiences and best practices of well-established CERT teams can serve as a valuable resource for the development of ICS-CERC.

ICS-CERC may require different resources and objectives, but they will have a common need to be built up based on good common practices from 'normal' CERT work.

ICS-CERC can be built up based on four main elements as explained below, which are in line with the baseline capabilities scheme[28]:

Table 1: Elements of ICS-CERC

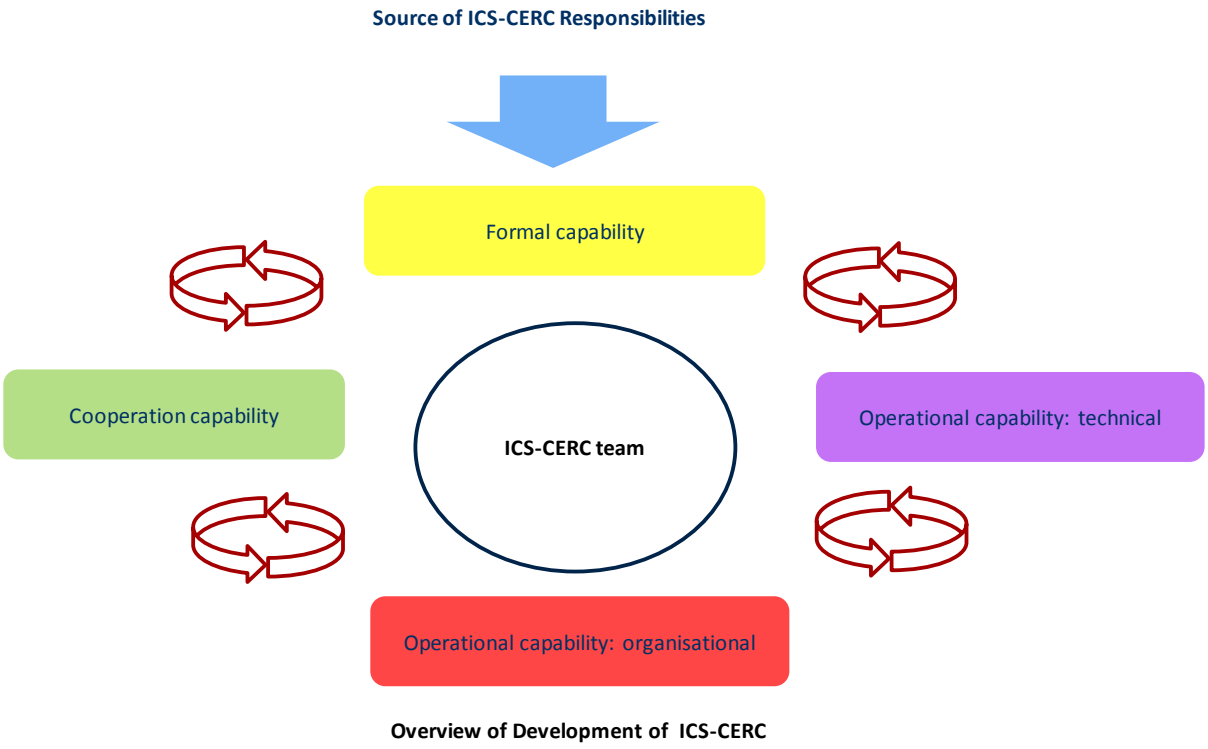
Element	Description
(1) Formal Capabilities (Mandate, role and responsibilities)	Covers the necessary processes and procedures concerning the functions, roles and responsibilities of actors as the ICS-CERC is being developed, what the mandate should include, how long the mandate should last, and why a mandate is important and needed.
(2) Operational Capabilities – Technical	Concerns the services and activities that an entity with ICS-CERC responsibilities should develop, the follow-up steps to developing these services, the investment required in terms of time and resources, and specifically how to develop incident response capabilities.
(3) Operational Capabilities – Organisational	Includes a working regime for entities providing ICS-CERC, developing the necessary internal expertise for ICS cyber-security, and training programmes and policies.
(4) Cooperation and Capabilities	Addresses stakeholders which the entities providing ICS-CERC should seek to cooperate with as the capability is being established and thereafter; describes why cooperation is necessary, and how to approach potential partners.

[26] It is important to note that even systems that are not connected to external networks can be targets of attack.

[27] By ICT environment, this document is referring to computers, computer networks, and other communications systems, but without a specific focus such as industrial control systems.

[28] ENISA, Baseline Capabilities for National / Governmental CERTs (2009); Deployment of Baseline Capabilities of National /Governmental CERTs: Status Report, 2012

Figure 1: Four main groups of CERC capabilities in ICS



2.1 Mandate considerations for ICS-CERC

A mandate for building ICS-CERC must clearly and fully cover functions, roles and responsibilities that fall under the four groups of ICS-CERC depicted in Figure 1. A mandate should take the nature of ICS cyber-incidents into account while respecting and ideally complementing a country's existing cyber-security structures and legislation.

2.1.1 Industrial Control Systems versus Information Communications Technology

ICS and ICT cyber-incidents can have different characteristics that should be taken into account as ICS-CERC services are being developed. As a fundamental matter, system performance (availability), confidentiality and data integrity are generally regarded as primary goals in the ICT world. Human and environmental safety are major considerations for ICS cyber-security providers due to the nature of the processes being controlled, although system availability and data and system integrity are also important.[29]

Furthermore, while cyber-attacks on both industrial control systems and ICT infrastructures can have significant and damaging consequences, industrial control systems are commonly associated with specific critical infrastructure sectors. The EC's 2008 Directive on European Critical Infrastructures establishes a procedure for identifying and designating European Critical Infrastructures and an approach for improving their protection.[30] As a result, ICS cyber-security can become more critical given the potential of many ICS cyber-security incidents to have a major impact outside of the ICT domain; for example, a cyber-attack on a power plant's control systems could cause a number of possible safety and health issues, whereas an ICT cyber-attack would be less likely to cause such issues (although it may do so depending on the sector attacked).

CERT respondent: "The very fact that the incident affects ICS and critical information infrastructure makes the incident severe and attaches high priority to its handling."

ICS responsibilities should be developed taking into account a number of factors that can distinguish ICS cyber-security efforts from traditional CERT capabilities, although it should be recognised that cyber-attacks on ICT can also cause significant harm and require development of robust capabilities:

Table 2: Distinguishing characteristics of providing ICS-CERC[31]

Distinguishing Characteristic	Example
Impact on supply chains, broader economy;	ICS cyber-attacks are more likely to cause significant damage due to the nature of the sectors where control systems are found. For example, a cyber-attack that takes an electrical power station offline, even for a limited amount of time, could

[29] See Guide to Industrial Control Systems (ICS) Security, Recommendations of the National Institute of Standards and Technology, US Department of Commerce, 2011 (available at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf)
[30] See Directive on European Critical Infrastructures, 2008 (available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF)
[31] See Guide to Industrial Control Systems (ICS) Security, Recommendations of the National Institute of Standards and Technology, US Department of Commerce, 2011 (available at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf)

	cause significant economic damage and create the potential for injury and/or loss of life.
Challenge of building ICS expertise and knowledge	Developing ICS-CERC requires attention to specific devices, protocols, and network infrastructures that may not be required for traditional CERTs. Further, cyber-security issues impacting control systems are more likely than broader ICT cyber-security issues to affect a specific sector, which makes it more challenging for ICS stakeholders to build up expertise and knowledge.
Challenge of finding qualified ICS employees	The fact that ICS cyber-security is often tied to a specific sector of CII can make it more challenging to find suitable and experienced staff for CERTs providing protection of ICS-CERC than for traditional CERTs, which are based more on general principles and skills.
ICS can involve extremely sensitive information	The sensitivity of information pertaining to ICS can make vendors and other ICS stakeholders less willing to share information about ICS cyber-security incidents, which in turn can make it more challenging to provide ICS-CERC services.
ICS cyber-security infrastructure is less developed than for ICT	There have been significant efforts to develop best practices across the ICT sector, ranging from transnational efforts such as FIRST to regional efforts such as Trusted Introducer or ENISA to national-level national / governmental CERTs. A number of organisations which are dedicated to improving ICT cyber-security exist, including sector-specific groups and ICS players such as US ICS-CERT, but such efforts are not as common or are in the early stages when it comes to ICS-CERC.

CERT respondent: "Despite bearing a lot of similarities with traditional IT systems, there are special ICS features … relating to a) network infrastructure; b) protocols; [and] c) devices. Ordinary CERTs do not possess the knowledge of how the infrastructures of ICS networks are organised, or how the protocols and devices work."

The process for building up ICS-CERC must take these factors into account, and these factors serve as the basis for managing a mandate.

2.1.2 Obtaining a mandate

A mandate should provide the basis for understanding what a team's responsibilities are when it comes to ICS-CERC. Having a clear mandate is fundamental for providers of ICS-CERC to gain the trust of constituents and other ICS stakeholders. This is particularly important in the ICS context for establishing the necessary levels of public-private cooperation (e.g., overcoming ICS vendors' hesitancy to share information with providers of ICS-CERC services due to their concerns about legal liability for improperly disclosing information).

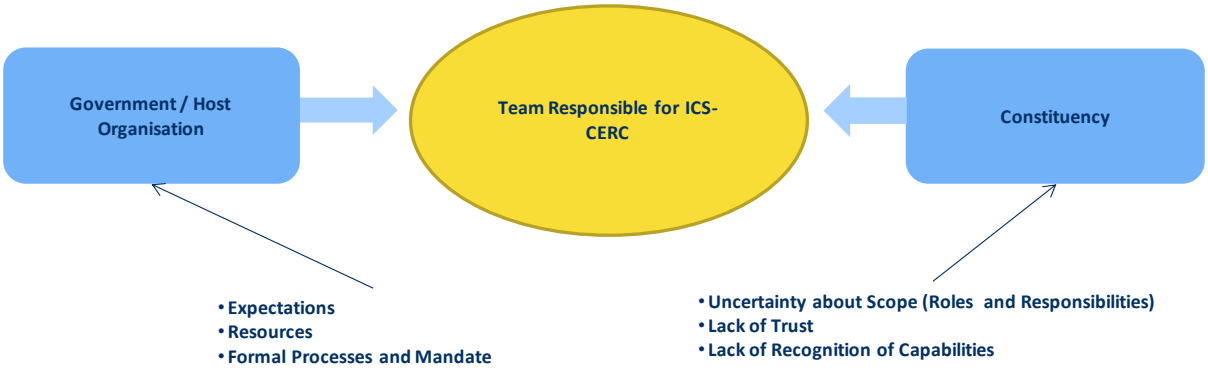
A number of factors must be taken into account while creating a proper mandate:

- A country's current cyber-security strategy (develop ICS-CERC in line with this)
- The mandate of the country's national / governmental CERT (develop the mandate advantageous to the development of ICS-CERC)
- Other existing regulations and communications regarding CIIP (proceed in line with European and national legislation in this area)
- The scope of mandates for teams already exercising ICS-CERC (learn from existing examples both in and outside Europe)
- The views of ICS stakeholders who will be part of the constituency regarding the scope of the mandate (engage these players while defining the mandate)

Consideration of the above-mentioned factors should help to ensure that an ICS-CERC mandate matches the needs of the constituency and the ICS community as a whole, and helps the CERT providing ISC-CERC services to establish and gain trust and legitimacy with both its constituency and other relevant institutions such as its government and the CERT community.

As mentioned before: ICS is a specific area with unique challenges, and it will be not easy for ICS-CERC to be developed in a way that meets the expectations of the organisations responsible for their development, of government, and of constituents. This suggests that ICS-CERC in a team should be developed with simplicity and directness in mind ("start small, think big").

Figure 2: ICS-CERC mandate considerations



Unfortunately, there are relatively few existing teams providing ICS-CERC services with publicly available mandates for use as a reference. ICS-CERT in the United States is one prominent example of a CERT that has been established to handle ICS cyber-security issues and has taken the lead in publishing best practices related to developing ICS-CERC.

A number of European CERT organisations have (to some extent) developed ICS-CERC and provide ICS cyber-security services to their constituents, including:

- ***CERT-FI*** (Finland),[32] which has an informal mandate in the area of industrial control systems cyber-security issues, and is hosted by FICORA, the Finnish national regulatory authority;
- ***Danish govCERT*** (Denmark),[33] which also has an informal mandate in the area of ICS cyber-security issues as an n/g CERT;

[32] See http://www.ficora.fi/en/

- ***Federal Office for Information Security*** (Germany),[34] which has a formal mandate in the area of ICS cyber-security granted to it by the German Parliament.
- ***CERT-PT*** (Portugal),[35] which provides some ICS-CERC services to its constituency despite having no formal mandate.

2.1.3 Range of the mandate

The range of the mandate for CERTs with ICS responsibilities also needs to be determined is the focus global, pan-European, regional, national or sectorial? ICS-CERC can be valuable at any of these levels. Each type of range has advantages and disadvantages:

Table 3: Potential range of ICS-CERC mandates

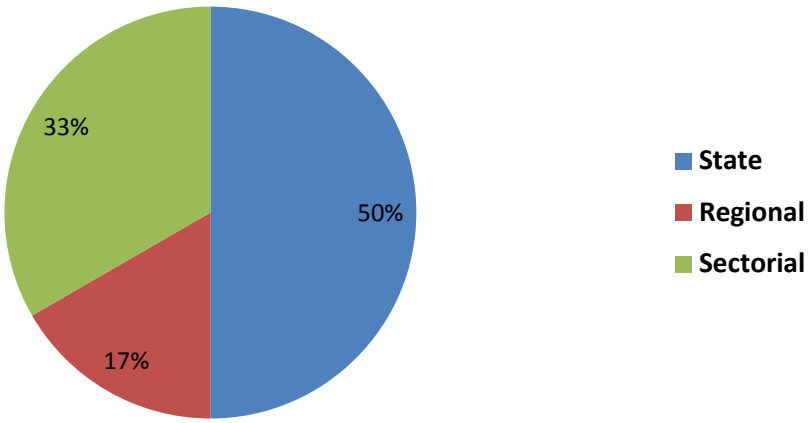
Range	Advantages	Disadvantages
Sectorial	Capabilities will serve sector-specific ICS stakeholders, and can easily develop into a forum for sharing of information and best practices given the constituency's common interests.	Can be more challenging to manage without a geographic component to the range; ICS stakeholders from different countries face different regulatory and legal environments; linguistic challenges can also arise.
National	ICS players from the same country will face common regulatory and legal environments; the focus on a single market makes it easier to focus on what types of ICS-CERC need to be developed.	ICS players might have little in common and little reason to cooperate besides sharing a common country; a national span makes it more important that the right entity is providing ICS-CERC to avoid political and other wrangling.
Regional / Pan-European	ICS-CERC with a regional focus can create synergies and facilitate information sharing across EU Member States; this can be positive for providing training, harnessing greater resources and providing services such as the gathering of statistics. The experience of institutions such as ENISA can also be leveraged to good effect. Further, private providers (companies) offering services in this area typically operate across borders in different countries, so cross-border incident management could be easier to implement from a practical perspective.	Regional-level CERTs with ICS responsibilities face challenges from different legal and governmental systems, which can make cooperation harder to achieve; ICS players might be more hesitant about sharing information in regional forums than in a national forum where there is clear responsibility for information security. Further, national governments often exert authority over CII, which can make it more challenging to establish effective regional or pan-European incident response capabilities for the ICS cyber-security arena.
Global	Global-level mandates for CERTs with	Global-level mandates can create

[33] See http://fe-ddis.dk/cfcs/CFCSDocuments/rfc2350_govcert.pdf
[34] See https://www.bsi.bund.de/EN
[35] See http://www.cert.pt

	ICSCERC responsibilities can create synergies, facilitate the sharing of good practices and information across the widest possible group of ICS stakeholders, and in principle offer access to greater resources, although obtaining those resources may still be challenging.	issues associated with regulatory and legal frameworks CERC. Furthermore national governments often exert authority over CII, which can make it more challenging to establish effective global incident response capabilities for the ICS cyber-security arena.

European CERT teams surveyed for the purpose of this document expressed a slight preference for mandate ranges of either national or sectorial level:

Figure 3: Preferred range for ICS-CERC, survey results



Number of answers=6 (Q: What is the optimal range of ICS-CERC?) (Graph shows results from survey asking European CERT actors with ICS-CERC responsibilities what in their opinion is the preferable range for a mandate in the field of ICS-CERC services)

It is worth considering whether dedicated ICS-CERTs should be created at Member State or EU level. The advantages of these types of state- or EU-level incident response capabilities dedicated to ICS cyber-security issues are clear: a state- or EU-level mandate would provide the chance for an organisation to develop ICS-CERC at a high level and establish a national-level (or higher) constituency. Available resources are a consideration for whether it makes sense to provide a mandate for developing ICS-CERC at these levels; if resources are limited, it may not be easy to argue persuasively for separating out a dedicated ICS-CERT instead of positioning it within a Member State or EU-level body with existing (traditional) CERT capabilities.

2.1.4 Defining the constituency

The constituency is the overall customer base to which a team with ICS incident response responsibilities provides its services. Ideally, the constituency should be defined as precisely as possible.

Within the ICS ecosystem, there are a number of types of players which are at the core of ensuring ICS cyber-security efforts, which should be considered when determining the constituency. A mandate can require ICS-CERC services to be provided to several types of stakeholders, including:

- ***Public ICS stakeholders***: ICS-CERC services will be offered to governmental bodies (assets owners), whether at a national level (e.g. national security) or more localised level (e.g. operations of specific plants). Generally, public institutions will be more open to cooperation with teams charged with developing ICS-CERC, and are likely to take a more cooperative approach. Stakeholders from public sector are at the heart of the ICS cyber-security ecosystem because many sectors with control systems fall within the public sphere and a government usually has a great interest in protection of its national CII.
- ***Private ICS stakeholders***: Private ICS stakeholders play an important role in the broader ICS cyber-security ecosystem in terms of incident handling. ICS-CERC services will need to be offered to companies (e.g. assets providers), so teams responsible for CERC providing them will have to invest more in relationship- and trust-building with these stakeholders, as they are usually more hesitant to share information or to report ICS cyber-security incidents. In order to reflect legal obligation for private stakeholders to cooperate with teams with ICS responsibilities, reporting of incidents needs to be formally defined in the mandate.
- ***ICS vendors***: (also part of the private ICS stakeholders, but due to their special role singled out in the considerations) ICS-CERC services will have to be offered to the companies that sell, install and maintain industrial control systems. These actors may even have their own ICS-CERC developed and therefore may be particularly reluctant to cooperate with other entities offering ICS-CERC services. ICS vendors are especially key constituents for teams with ICS-CERC responsibilities because of their important roles in terms of providing asset owners and providers with service-level agreements (SLA), vulnerability patches, updates, and upgrades of systems.

Teams offering ICS-CERC services may decide to limit them to constituents of a certain sector or to a particular company's customers. If the scope of a mandate is limited in such a way then it is important that it covers all the key players (public actors, private actors, ICS vendors) within that sector. Likewise, care should be taken that a mandate is not too broad as to make the constituency completely unwieldy. When a mandate covers multiple or all CII sectors, it should be also considered how to involve all stakeholders from all of these sectors in defining the mandate and considering the services and role of the team with ICS-CERC. This is particularly challenging due to the different nature of sectors (for example “energy” and “health”).

2.1.5 Seeking input for mandate

Teams responsible for developing ICS-CERC services need to investigate to third parties for input regarding their mandates and development of capabilities. As mentioned, there are still very few organisations offering ICS-CERC services or ICS best practices in comparison to more general, CERC traditional CERTs, but input from other parties is invaluable.

There are a number of organisations with worldwide, European, national or sectorial scope that could offer input to a team seeking to develop ICS-CERC services. These include[36]:

- *CIGRE*: A global organisation dedicated to the exchange of information and best practices about power stations.[37]
- *International Atomic Energy Agency*: The IAEA offers meetings and good practices related to the security of nuclear energy facilities.[38]

[36] For an extensive list of ICS security-related initiatives see the Annex IV of ENISA report ‘Protecting Industrial Control Systems: Recommendations for Europe and Member States’, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/annex-iv

[37] See http://www.cigre.org/What-is-CIGRE/Activities

- *ENISA*: The European Network and Information Security Agency provides a variety of best practices regarding ICS cyber-security as well as recommendations and good practices for establishing incident response capabilities in Europe.[39]
- *ESCoRTS*: The European Network for Security of Control and Real Time Systems aims to foster progress towards cyber-security of industrial control systems in Europe by assisting the EU as a whole (e.g. authorities, industry, manufacturers, etc.) in developing informed positions and in shaping current and future efforts related to control systems security standardisation.[40]
- *European Network for Cyber Security*: The ENCS is a cooperative association that creates and brings together knowledge and resources to secure European critical infrastructures.[41] [42]
- *ICS-CERT*: The US ICS-CERT is widely regarded as the leading dedicated ICS-CERT worldwide, and offers a variety of resources including good practices and training materials, as well as significant experience in providing ICS-CERC to its constituency.[43]
- *Centre for the Protection of National Infrastructure*: The United Kingdom's CPNI provides protective security advice and advice for security planning.[44]
- *US Department of Energy*: The United States' DoE offers a variety of documents and good practices for ICS-CERC.[45]
- *US Department of Homeland Security*: The DHS provides recommended practices with regard to ICS security and is the host organisation for US ICS-CERT.[46]
- *Institute of Electrical and Electronics Engineers*: The IEEE produces a significant amount of literature on engineering-related topics.[47]

All of these organisations could be sources for teams charged with developing ICS-CERC services as they try to establish a mandate and promote their CERC services to their constituencies

2.1.6 Importance of mandate

The current practice in Europe is that national / governmental CERTs responsible for providing ICS-CERC services are not given a formal mandate. Instead, they are often provided with a broader mandate that covers all of their activities (including ICS-CERC services) to the extent that they are "expected to develop" the capabilities. This may reflect the extent to which ICS-CERC services are still viewed as just an extension of these n/g CERT teams' core responsibilities, rather than as an area which requires the development of a separate group of capabilities.[48]

This approach may work for some teams' CERC, but it can also create challenges for them if their CERC mandate is not specific enough to support cooperation between them and their private sector constituents. This could be especially challenging for teams responsible for developing ICS-CERC when an existing entity already provides ICS-CERC services. This may occur if an entity plays a larger role in cyber-security in the country and has also other responsibilities. In particular, mandatory

[38] See http://www.iaea.org
[39] See http://www.enisa.europa.eu
[40] See ESCoRTS, Security Control and Realtime Systems, Survey of Existing Methods, Procedures, and Guidelines*, available at* http://www.cen.eu/cen/Sectors/Sectors/ISSS/Focus/Documents/D21.pdf
[41] See https://www.encs.eu/
[42] See https://www.encs.eu/
[43] See http://ics-cert.us-cert.gov/
[44] See http://www.cpni.gov.uk/
[45] See http://www.doe.gov
[46] See http://www.dhs.gov/
[47] See http:www.computer.org
[48] Analysis based on the survey conducted to provide input into this document.

reporting requirements to such entities may conflict with the more voluntary model of cooperation favoured by teams with ICS-CERC, especially with private actors and ICS vendors.

As discussed previously in this study, the nature of ICS cyber-security threats and the potential reluctance of private-sector ICS players and vendors to cooperate with teams with ICS-CERC make establishing a baseline supporting cooperation especially important. Thus, a team charged with developing ICS-CERC services that does not have a clear mandate may struggle to achieve trust, legitimacy and cooperation with key ICS stakeholders.

In the longer run, having a formal mandate for ICS-related activities will benefit teams because it will offer a clear and specific commitment to their responsibilities and how they should interact with the various ICS stakeholders. In addition, having a formal mandate means having formal legislative and legal support for the activities of a team with ICS responsibility. In turn, with formal processes in place that must be respected, ICS-CERC services must be developed within certain guidelines. The increasing prominence of ICS cyber-security matters will make it more worthwhile to ensure that teams with ICS responsibilities have a clear mandate for these activities and the necessary support and tools to carry them out.

2.2 ICS operational capabilities: Technical considerations

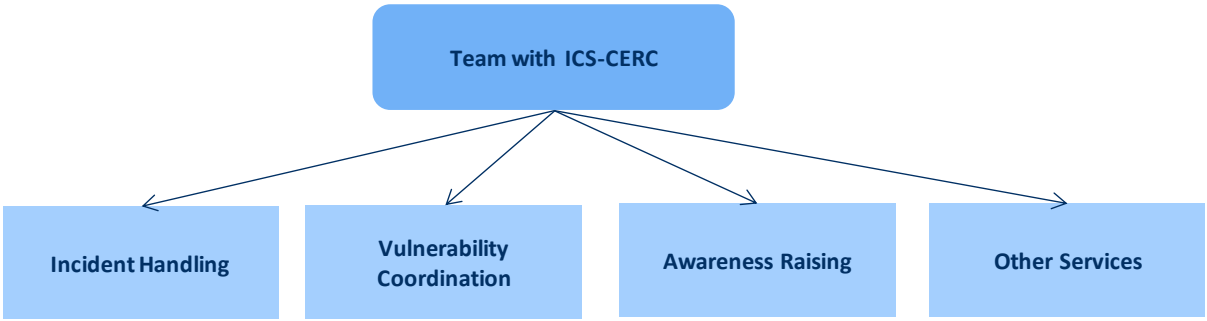
When building up operational capability, one main challenge is to determine, to which ICS-CERC services are suitable for the constituency. This decision must be supported by a good understanding of the constituency size, type of services which could be delivered, resources available, and, last but not least, the scope of the mandate.

Services provided in the initial stage of such a development of ICS incident response capabilities will depend on a number of factors, including:

- The mandate and mission;
- Available resources (human and financial);
- Size and scope of the constituency and its needs;
- The current services provided by the team outside the ICS constituency (synergies).[49]

Current practice shows that teams aiming at establishing ICS-CERC services typically provide several other CERT services as well: reactive services, proactive services, and management services with a focus on incident handling, vulnerability coordination, raising awareness among constituents, and training.[50]

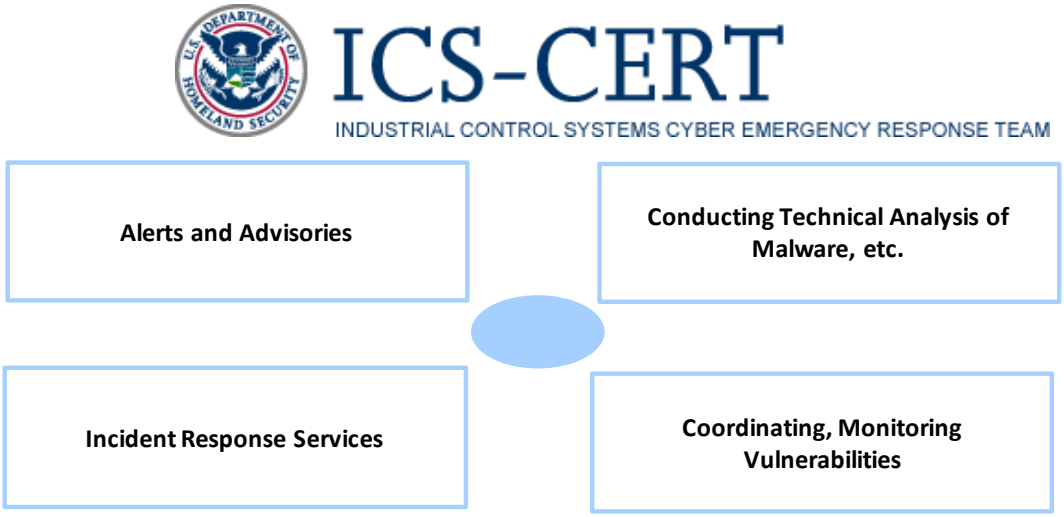
Figure 4: Services portfolio for ICS constituency



Within these categories of services, teams can offer any number of more specific ICS-related services. For example, US ICS-CERT provides four core areas of functionality to its constituents:

[49] Valid only if the CERT is already mandated with building ICS incident response capability.
[50] Results of survey of European CERT players carried out in conjunction with this document, asking those with ICS-CERCs about the specific types of ICS services they offer to their ICS constituencies.

Figure 5: US ICS-CERT service offering[51]



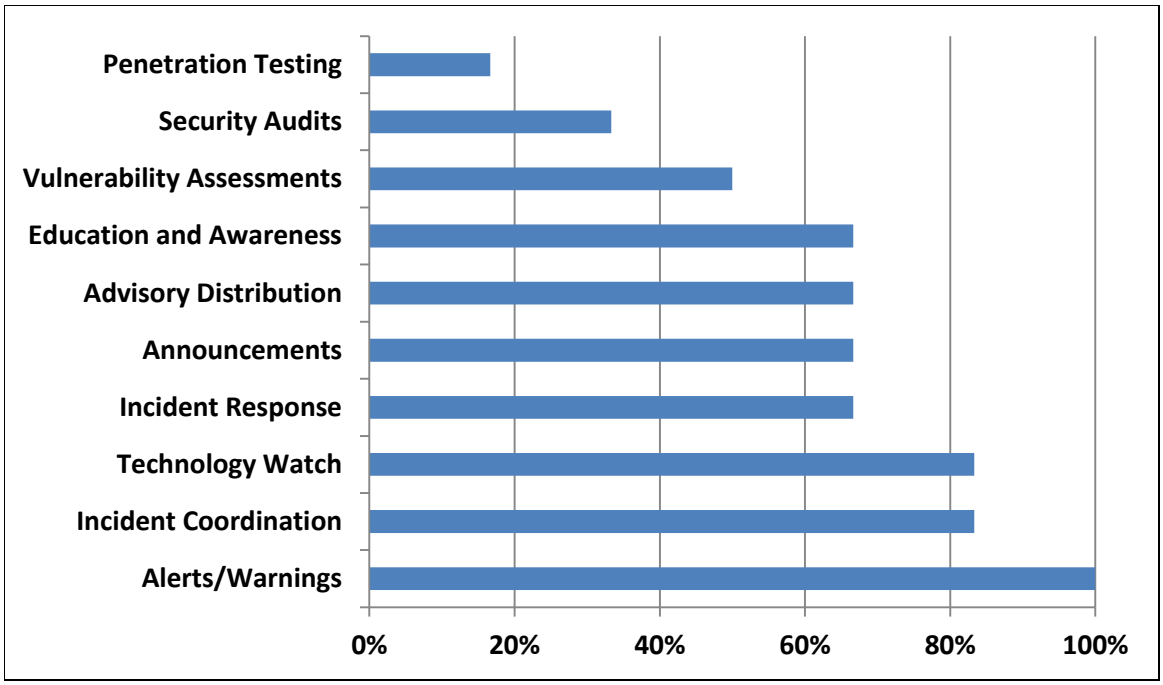
In 2013 JP-CERT, which was charged with building ICS incident response responsibilities recently, provides three ICS-related services: incident handling support, vulnerability coordination and awareness raising for ICS assets owners.[52] The team intends to improve its incident handling capabilities and is considering providing on-site and off-site services to ICS asset owners in the future.

Figure 6: JP-CERT ICS service offering[53]

Interestingly, current practice in Europe shows that teams with ICS-CERC responsibility do not universally provide either incident response service or vulnerability assessments for ICS, even though these are generally considered to be core services of any CERT team.[54] On the other hand, many of these teams with ICS-CERC provide more 'passive' services such as issuing alerts, incident coordination, and technology watch. This may reflect strategic decisions by these teams to establish themselves by first developing their capabilities in easier-to-provide services or it may suggest that these teams have limited resources (financial and personnel).

[51] ICS-CERT Year in Review, 2012, U.S. ICS-CERT, at p. 3
[52] See http://www.jpcert.or.jp/english/cs/controlsystemsecurity.html
[53] See http://www.jpcert.or.jp/english/cs/controlsystemsecurity.html
[54] Analysis based on survey conducted in conjunction with this report

Figure 7: Services provided by CERT respondents providing ICS services



Number of answers=6

Q: What services, if any, do you provide in relation to ICS?

It is crucial that the teams with ICS responsibilities decide on offering services only after having discussed with their constituents (ICS providers/asset owners) and ICS vendors (see also section 2.4 on cooperation). At the moment it is problematic that IT security vendors often have insufficient understanding of ICS environments when they are trying to sell their products. According to ICS security experts, vendors often try to apply security designed for protecting data in a traditional ICT network, which has many aspects not applying to a network of ICS devices. For example, in the ICT network environment a malware-infected computer is often simply taken off the network. The same approach in an ICS environment could potentially lead to a catastrophe in a power plant, manufacturing facility or oil and gas pipeline. Therefore, SLAs must be given a strong priority with regard to vendors.[55]

2.2.1 CERT services to develop good technical capabilities for ICS

Even after taking into account the differences between ICS and ICT, teams developing ICS-CERC still have to decide what services they will provide to their constituency. This section provides a brief overview of some of the services that are and can be provided in the ICS area. It also explains how the nature of ICS cyber-security influences these services, and looks at current practices from existing teams to deliver services in ICS area.

[55] For more information see the article 'IT security vendors seen as clueless on industrial control systems' (http://www.csoonline.com/article/733873/it-security-vendors-seen-as-clueless-on-industrial-control-systems)

2.2.1.1 Incident handling

Incident handling is a core service that every CERT must provide, and should also be considered a core service in the ICS area, even though incident handling services in the ICS context are often challenging to develop (as mentioned before). Some reasons for this being a challenging task include for example the difference in type and priority of incidents, different standards and procedures to deal with and manage them, the type and size of the network and (national, regional or global) distributed network nodes (ICS objects).

Often ICS-networks are autonomous, completely separated or stand-alone, sometimes distributed systems across the network (with different ICS/security solutions and vendors), following different legal regulations, policies and strategies across the national borders. In addition, what counts as an incident handling service can be perceived differently by different actors, e.g. as incident response, coordination, on-site support, or advisory services. There are also other aspects to consider while deploying ICS-CERC as mentioned at the beginning of this chapter: the scope of the mandate and current services provided by the existing team or requirements for the personnel.

There are several problems that can arise in the context of incident handling that can be specific to the ICS arena, and in particular tend to affect parties' willingness and ability to share information with a team responsible for incident handling in this area:

- Concerning ICS vendors: obtaining timely information about ICS incidents, vulnerabilities and patches could be challenging if it is not clearly defined in SLAs for specific ICS products;
- Concerning ICS providers /ISPs: ICS cyber-security incidents are sometimes not discovered in a timely manner due to providers' lack of proper security detection capacity;
- Concerning ICS asset owners: there could be a lack of trust or willingness to cooperate especially if the team's responsibilities (mandate) are not clearly identified (e.g. necessity of reporting incidents in CII area).

There is broad agreement that there is not yet sufficient sharing of information about ICS cyber-security events. Still there does not seem to be significant support for mandatory reporting of ICS incidents affecting critical infrastructure by ICS providers (or other actors) to governments or other entities with ICS-CERC responsibilities. This makes it more complicated to carry out ICS-CERC responsibilities, and should be taken into account by teams trying to develop strategies for deploying their capabilities with these players.

The problem of encouraging parties to share information makes it more important that teams with ICS responsibilities know which parties to turn to when handling incidents:

- ***CERTs*** offer advisories about emerging security risks or about incidents seen elsewhere[56];
- ***Vendors*** offer security patches and updates, and are good resources for general information about ICS technologies and equipment;
- ***ICS Asset owners*** should be involved in discussions about how to improve their business models, which includes taking into account obtaining ICS cyber-security services;
- ***ICS Service providers/ISPs*** should share information about network outages and cyber-security incidents and can help minimise the impact of these incidents to the extent possible;
- ***Other teams with ICS-CERC*** can be valuable in terms of obtaining information about challenges they have faced and best practices, as well as potential cooperation in terms of responding to a particular incident.

[56] In Europe provided for example by CERT-FI or CERT-BUND.

Teams with ICS-CERC responsibilities need to take on the challenge of growing into a trusted partner to these other types of players when it comes to the incident handling service provision. Reluctance to share information about incidents will be a constant challenge for any team mandated with ICS incident response capabilities.

Respondent from the ICS sector: "The main hindrance [to effective incident handling] is the possibility of being heavily penalized for disclosing such information, which results in loss of credibility and value for the company. The way to overcome this would be to establish a non-governmental (CERT) entity dealing with ICS incidents."

CERT respondent: "It is important that ICS vendors, operators, and ISPs are all involved in the incident handling process. Vendors often do not disclose all information, although they have to provide patches and work on mitigation of the incident. Operators tend to ask CERTs for assistance. Therefore, CERTs are perfectly fit to act as an intermediary and coordinator of incident handling management."

The incident handling process should involve as many of the parties discussed above as possible, including ICS vendors, operators, and service providers, as well as the impacted party and the ICS-CERC team. Because of the challenges involved with incident handling, it is an area in which teams with ICS-CERC responsibilities can demonstrate their value, importance and experience to their constituents. Thus, it is very important that they develop strong and consistent incident handling capability in the area!

As mentioned previously, ICS incident handling service could encompass a number of actions:

- Providing technical support to the victim of an attack;
- Guiding the attack victim to recovery;
- Developing a process for protection in the event of similar future attacks;
- Alerting other potential attack targets without disclosing confidential information;
- Assessing and relating the incident to other events (with the help of authorities).

Another challenge teams with ICS CERC responsibilities face is that some ICS asset owners do not have well defined cyber-security incident response processes in place.

Incident Detection

An initial task for teams responsible for providing incident handling service is to acquire information about an on-going cyber-incident affecting an industrial control system. There is usually no legal responsibility for ICS asset owners, vendors, or network service providers to report incidents, and these players may not be comfortable with sharing this information.

This makes it important for the teams with ICS responsibilities to demonstrate trustworthiness and transparency and instil confidence in their abilities to handle data and information with sufficient confidentiality.

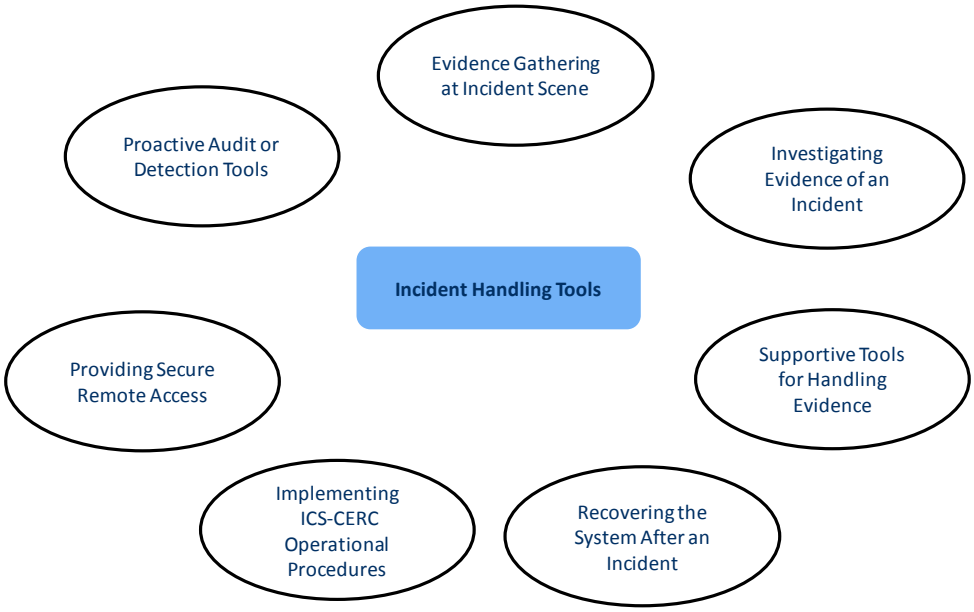
There are a number of steps that can be taken to make it less burdensome for the players to share information.

- **Incident detection services (on the site of asset provider)**: Incident detection is usually within the responsibility of the ICS asset provider. The incident detection infrastructure should be in place on site of these stakeholders. A team with ICS responsibilities can provide advice about the security settings (risk assessments, if needed, for example)
- **Incident verification**: A team with ICS-CERC needs to be able to verify that an incident is on-going by discussing it with the reporting party and through data analysis. Current practice is to use various means of communicating with other players, including SSL-protected websites, PGP-encrypted emails and telephone calls.[57]
- **Acquiring data**: It is important that teams offering ICS-CERC services have the correct and complete set of data about an ICS cyber-security incident to respond appropriately. Common data points that should be collected include: the type of ICS incident (accident, virus, etc.), data about the possible attacker, the system and hardware impacted, a brief incident description and the incident's impact. It is advisable that teams follow common CERT incident reporting formats with adjustments for ICS incidents.
- **Coordination**: Coordination is an important element of efforts to respond to detected ICS incidents. Teams with ICS-CERC should coordinate with a variety of players, including: the impacted ICS organisation, the team's own host organisation, vendors, operators, network service providers, or relevant governmental bodies. Contact information should be regularly checked and updated. It is also important that teams developing ICS-CERC disseminate their contact information on a regular basis to their constituency.
- **Incident response tools**: A team with ICS-CERC responsibility has to have the necessary tools to handle an incident. For traditional CERTs, ENISA has grouped tools into seven functional groups, which also make sense for ICS cyber-incident response efforts, given that interviewees say that the processes for responding to an ICS incident are generally similar to those for an ICT incident.[58]

[57] The practice also shows that ICS players (providers or owners) are not very familiar with, or equipped with, the security level of communication (e.g. PGP encryption).

[58] For more information see ENISA's Clearinghouse for Incident Handling Tools at http://www.enisa.europa.eu/activities/cert/support/chiht

Figure 8: ICS incident handling tools[59]



Note: Activities related to detection of an ICS incident are usually the responsibility of the ICS provider. That is why the teams with ICS-CERC services could have, for example, an advisory or coordination role in this regard (it usually doesn't have the access to the network itself.)

Incident Containment

At this stage, the teams with ICS-CERC need to take an active part in the whole process of incident management. They especially need to assess the impact of the incident on the critical infrastructure in the country and ensure (in collaboration with the ICS asset owner or provider) that the incident does not spread further and avoid greater damage.

Once information about an ICS cyber-security incident has been obtained, the necessary steps must then be taken to respond to the incident, according to the initial priority of the incident. The initial priority has to be assigned by an ICS incident reporter such as a system administrator of a particular industrial control system (following defined incident categorisation policy). Then, based on more general knowledge or incident escalation procedure (e.g. other ICS providers are complaining about identical/ similar incidents) the priority can be changed/ raised.

Containment can be especially important in the industrial control system environment because of the special considerations associated with ICS security, including among others[60]:

- ***Performance requirements***: Industrial control systems are time-critical by nature in terms of the levels of acceptable delay and jitter, which means that attacks on ICS need to be contained as quickly as possible.
- ***Availability requirements***: ICS processes are often continuous in nature, which means that there cannot be outages or that outages should be planned in advance.
- ***Risk management requirements***: ICS cyber-security incidents can threaten human life and injury, endanger public health or confidence, raise regulatory compliance issues, and cause

[59] http://www.enisa.europa.eu/activities/cert/support/incident-management (Section 8.9)
[60] National Institute of Standards and Technology, US Department of Commerce, Guide to Industrial Control Systems (ICS) Security, Section 3-1 (2011)

the loss of equipment or valuable intellectual property, all of which make containment critical.

As a result, the necessary steps to prepare to respond to incidents must be taken. In particular, processes and policies are needed for:

- ***Handling evidence***: The nature of ICS cyber-security incidents [61]means that evidence will have to be handled which is confidential, sensitive, or proprietary in nature. Thus, consideration must be given about how to handle such evidence so as to not lose the support and trust of constituents.[62]
- ***Documentation***: Incident response processes need to be documented properly. This is important both for confidence and capability building, and also helps prepare records for analysis and lessons learnt from previous cases.
- ***Role distribution***: Effectively containing an ICS incident means having well-defined roles and responsibilities among different players that are involved and responsible for the successful containment.

Incident Remedy

Remedial actions for an ICS cyber-security event should include mitigating the incident's short- and longer-term impact on the affected organisation, escalating the response as necessary, and ensuring that the right lessons are learned so that the same incident does not happen again. As with other aspects of responding to ICS cyber-security incidents, the nature and the possible criticality of ICS cyber-incidents should be taken into account when the incident remedy or escalation procedures are being set up.

Mitigation is generally a core objective of remedying an incident. Impacted ICS providers mostly escalate the incident only when it is severe enough to seriously affect their production. So the remedy depends on several aspects, for example on the incident severity (affecting energy supplies, transport flows or even people's lives), criticality of the system, nature of the intrusion (large-scale DDoS attack), etc. Incident mitigation can be a core activity that can help to both minimise an organisation's loss and mitigate the weaknesses that the attacker exploited.

In order for this service to bring real benefits to the constituents, it is important that the necessary arrangements are made on the part of interested stakeholders. Teams need to have in place resources and an operational mode for responding to and mitigating the impact of ICS incidents. The ICS providers need to have effective mechanisms and processes for incident detection and potentially sharing of the incident data with ICS-CERC teams. The ICS vendors also have an important role to play: to provide patches and improvements to their solutions in line with evolving nature of cyber-attacks on ICS. As a result ICS and the infrastructure need to be configured correctly (hardening) and access rights need to be assigned adequately.

Due to the nature and potential consequences of ICS cyber-security incidents, responses to incidents may need to be escalated either within their host organisations (company) or to the appropriate reporting bodies (e.g. governmental entity responsible for cyber-security over CIIP, if applicable). The nature of threats to industrial control systems might have a huge impact on different assets. When public safety or environmental damage is at issue, remedying the incident or preventing

[61] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents

[62] For example, it concerns evidence handling of the Indicators of Compromise (IoC).

worse case scenarios from occurring will mean bringing other parties into the discussion. As with other aspects of ICS cyber-security responses, this means that there must be a plan in place for escalating the response to an incident before it causes great damage.[63] [64]

Remedying an ICS cyber-security incident also means not allowing it to happen again. There is both an information sharing and analytical side to this. It means having procedures in place for sharing information about cyber-incidents, while taking into account legitimate confidentiality concerns of ICS organisations, vendors, and other impacted players. One of the formats used for automatic sharing of information on incidents in a unified way is OpenIOC.[65]

Incident Closure

Closing off an ICS cyber-incident is the last step of the incident handling process. Some aspects of incident closure (such as artifact handling, etc.) may be difficult to provide due to lack of resources. Even within the 'traditional' CERT community many national and governmental CERTs do not offer artifact handling services.[66] Thus, cooperation with the host organisation and reaching agreements with sources of funding will be an important part of efforts to develop these specific services. The importance of for example artifact handling services should not be underestimated, as they can help to understand why an ICS cyber-security incident occurred (and, in consequence, prevent it from happening again.

Other aspects of incident closure, including dissemination of 'lessons learned', are less resource-intensive, but still require the investment of time and manpower to be planned and implemented. The incident closure has to be closely coordinated among teams with ICS responsibilities and ICS providers (doing follow-up onsite modifications to their ICS like reconfiguration). ICS vendors need to be involved after lessons have been learned, in order to upgrade and modify ICS solutions and become more resilient to cyber threats.

It is important that teams with ICS responsibilities keep records of ICS incidents and provide periodic summary reports. These summary reports are a valuable source for updating national cyber-security strategies in general and strategies for critical (information) infrastructure protection in particular. On a European level it would be useful to have overall European statistics on ICS security as well. These could take a similar form to that used for reporting 'Article 13' incidents in the Member States.[67] Providing comprehensive statistics will be welcomed by ICS-CERC teams, vendors, providers and asset owners alike, which have up to now relied mostly on reports from ICS-CERT in the US.

2.2.2 Maturity of capabilities and further improvement of operational services

Consideration should be given at an early stage as to how to improve and further develop technical capabilities (service portfolio) once a team responsible for developing ICS-CERC is off the ground. The shifting nature of cyber-threats facing industrial control systems necessitates this, as does the fact that constituencies will expect more as they feel more comfortable in their cooperation.

---

[63] One recent example of such a disaster recovery plan for critical infrastructure: http://www.state.il.us/iema/disaster/pdf/IDRP/IDRP_AnnexH.pdf

[64] Detailed information on ENISA's work in cyber crisis management and national contingency plans is available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation.

[65] http://www.openioc.org/

[66] See conclusions of ENISA's report on Baseline Capabilites of national/ governmental CERTs: http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012

[67] See ENISA's Annual Incident Report 2011 report: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

Further development of ICS-CERC should consider two main areas:

1. Deepening and improving services already offered. In particular, this will mean refining and improving the processes for handling ICS cyber-security incidents, as this is a core service to provide.
2. Broadening the scope of services offered. Constituents will want more services as they grow comfortable with the roles of ICS-CERC available to them, whether these services are in areas such as providing training courses or beginning to offer specific services (e.g. artifact handling) associated with the incident handling process.

2.3 ICS operational capabilities: Organisational considerations

Operational considerations for teams with ICS capabilities should focus on making sure that the right support is in place for the ICS-CERC services, including having the right personnel, providing training that reflects the ICS environment and ensures that staff have the right skills and knowledge, and working with the host organisation to make positioning of the ICS capabilities as beneficial as possible.

2.3.1 When to provide services for ICS – which operational mode to choose?

As is the case for CERTs dealing with 'traditional' ICT systems, teams with ICS responsibilities must consider incident handling to be a core service, to an even greater extent because ICS failures resulting from attacks, human errors and other causes often have immediate effects on assets and potentially lives. Examples include energy catastrophes such as oil spills, floods, leakages of dangerous chemicals, major rail incidents, or power outages. Therefore, a 24/7 reachability regime for incident reporting and handling is a necessity for this part of reactive services, because of the possible critical impact of an incident occurring in the ICS environment.

However, for the other groups of services provided by CERTs (proactive services and security quality management services[68]) the operating regime can be business hours only. In the case of some services like technology watch, the operational regime could be defined and agreed in cooperation with private companies, including ICS technology vendors.

When deciding upon the operational mode, it is important to consider whether such a model is already in place at the team entrusted with providing ICS-CERC services or whether this will need to be built up from scratch and with additional resources. There is also the need for ICS-CERC teams to determine whether existing CERT IT software and solutions can be applied to ICS-related incidents. For most of the typical CERT services this can often be the case, only for specific services like penetration testing or reverse engineering the settings might be different.

Last but not least legal aspects have to be taken into account. This may prove the most challenging task as protection of ICS is related to national security matters and the legislation in this area is very specific – as is the accompanying information process, which is usually highly sensitive.

2.3.2 The right personnel for the ICS environment

Having quality staff is critical for developing and providing ICS-CERC services. Human resources requirements will depend on factors such as mandate, constituency, available resources, regulatory and business drivers, and operational hours. Staffing correctly means finding individuals with the right experience and capabilities as well as reaching a size sufficient to carry out the mandate.

In terms of division of responsibilities and roles, there are different potential team sizes and divisions of responsibilities that can be used. The structure to be used by a particular team should be based on considerations such as its mandate, its host organisation, the services it is providing, resources available to it, and the services that it plans to provide in the future. For example, when an incident handling service in a particular operational mode is being offered, personnel and resources must reflect this. Moreover, it should be kept in mind that as ICS capabilities are in the early stages of being developed, resources and personnel may need to be distributed differently than when higher levels of operational maturity have been reached.

There is no one solution for dividing staff's responsibilities that will suit every team with ICS responsibilities. As a general matter, there are additional specifications to the ordinary CERT team

[68] For a detailed definition of CERT/CSIRT services see: http://www.cert.org/csirts/services.html.

composition (e.g. for CIIP strategy and policy as well as ICS risk analysis and contingency planning), as these are core matters where ICS-CERC are being created. Beyond this, technical expertise with ICS skills and knowledge will be needed to ensure that incident handling and other services related to ICS can be provided at a high level.

The general process for hiring staff for developing ICS-CERC services will be similar to that for traditional CERTs, but the specificity of the ICS context should be kept in mind. In particular, staff for teams with ICS-CERC responsibilities should have specialised knowledge and skills that relate to the aspects of providing ICS cyber-security capabilities discussed previously in this document. Most important for developing ICS-CERC will be reaching a base level of staffing either with these skills or of individuals who are capable of obtaining the skills to provide the ICS-CERC services to be offered.

CERT respondent: "There are very specific knowledge domains associated with control systems versus commodity cyber infrastructure. Not only technical, but business knowledge as well. It is important to understand the economic drivers of an industrial sector in order to effectively work with them to improve their cyber security."

CERT respondent "Despite bearing a lot of similar characteristics with traditional IT systems, there are special ICS features that incident handlers must be knowledgeable of."

Respondent from ICS sector: "While, for example, forensics analysis is the same, ICS incident handlers must possess the knowledge and capabilities to deal with specifics of PLC and RCU."

The hiring process for staff on teams responsible for developing ICS-CERC is an important matter that should be given sufficient consideration. In particular, the process should acknowledge the fact that staff will be dealing with CII matters and helping ICS players handle incidents that have the potential to cause significant damage. This means that staff should be vetted thoroughly during the recruitment process, and consideration should be given to factors such as individuals' ability to perform under pressure and willingness to be on-call for incident handling and response at non-working hours. This is important not only for the development of ICS-CERC on a team, but also for making sure that ICS vendors, industry players, and even governmental agencies are comfortable working with the team as it establishes ICS-CERC services.

Pre-employment screening methods provide a good tool for the hiring process. Pre-employment screening is a type of check that employers conduct either before they offer a candidate a job or during the hiring process. The types of screenings include criminal background checks, credit checks, employment history verification, education verification, and driving record checks or other specific on-demand checking. However, this pre-employment screening should be done only for pre-selected candidates fulfilling the main requirements: the technical knowledge and experience. In some cases

[69] http://en.wikipedia.org/wiki/Programmable_logic_controller
[70] http://en.wikipedia.org/wiki/Remote_Terminal_Unit

additional certificates might be requested (e.g. allowing access to confidential information), which are issued by authorised bodies (usually ministries of the interior/home offices).

It must be decided whether an existing team should be commissioned with developing ICS-CERC services or a new team should be set up for this. Staff from existing CERTs can be entrusted and appointed, particularly for matters which are not necessarily ICS-specific, including the typical CERT operations and capabilities related to distributing information. The use of and sharing of staff between teams is desirable from several perspectives, including cost-saving, administrative knowledge sharing, and building capital for the team with ICS-CERC at other organisations.

2.3.3 Training personnel for the ICS environment

Training for ICS environments should be given significant consideration, as it is a core part of efforts to develop ICS-CERC services. The first matter to be considered is who can be offered training. Of course, teams with ICS-CERC will need to offer sufficient training opportunities, but they should also consider working with other members of the ICS community when it comes to training. For example, ICS vendors, asset owners, and providers all need continual training as well to keep their staff up to date on ICS cyber-security matters. Thus, it will often make sense for teams developing ICS-CERC services to collaborate with these stakeholders, which creates mutual benefits. Collaboration can be useful in creating the type of ICS-holistic grounds for discussion that could have significant benefits not only for the team with ICS-CERC services in developing its capabilities but also for helping to build cooperation between it and ICS players in its market.

Beyond an ICS-specific view, teams with ICS-CERC responsibility can also consider whether cooperation with established CERTs could be useful in providing training. The 'traditional' CERTs are often better established, have longer track records of offering training to their staff and constituents, and may have more resources. Of course, this cooperation will typically be most fruitful in areas where ICT and ICS activities and services overlap, but CERTs may find that their staff also benefit from building up knowledge about industrial control systems. This is especially the case where the ICS agenda falls under one team's responsibilities.

The specific nature of providing ICS-CERC services has to be considered, though. In particular, the impact of ICS cyber-security incidents can differ, as discussed in this document, and the methods to be taken to mitigate these impacts will be different as well. Moreover, the ICS technical environment is often an autonomous, internal network, which means that cyber-security threats can show different characteristics from conventional ICT systems and networks. There are also software- and hardware-specific protocols that are used for ICS, and training for ICS cyber-security capabilities has to take these specifications into account as well. These factors can make it more challenging to provide training in the ICS area than in the traditional ICT domain.

As a result, training opportunities for staff must be constantly sought out by teams responsible for developing ICS-CERC services, especially when resources are limited. Cooperation with CERTs and other organisations which provide training in this area can lower the costs of the actual training, as can virtual training programmes. For example, the SANS institute offers a number of virtual training programmes in the ICS area, which could either be used by teams with ICS-CERC responsibility or as a basis for developing similar offerings.[71] ENISA also provides extensive online training material for CERTs including virtual images, handbooks and toolsets for students and lecturers.[72] This training and exercise material is provided free and can, on request by a EU Member State, be applied by ENISA trainers.

[71] See http://www.sans.org/vlive/sessions
[72] http://www.enisa.europa.eu/activities/cert/support/exercise

2.3.4 Suitable hosting organisation for ICS incident response capabilities

The host organisation has a strong influence on the development of ICS-CERC, because its power and position in the national CIIP policies and processes can streamline measures aimed at enhancing cyber-security. It can also allow more flexibility when dealing with incidents (e.g. escalation procedure). It can be considered as an advantage if the host organisation of a team with ICS responsibilities has an important position as regards planning and execution of national policies in CIIP. This is especially true while escalating incidents, when a direct line of communication to national bodies responsible for CIIP plays a crucial role.

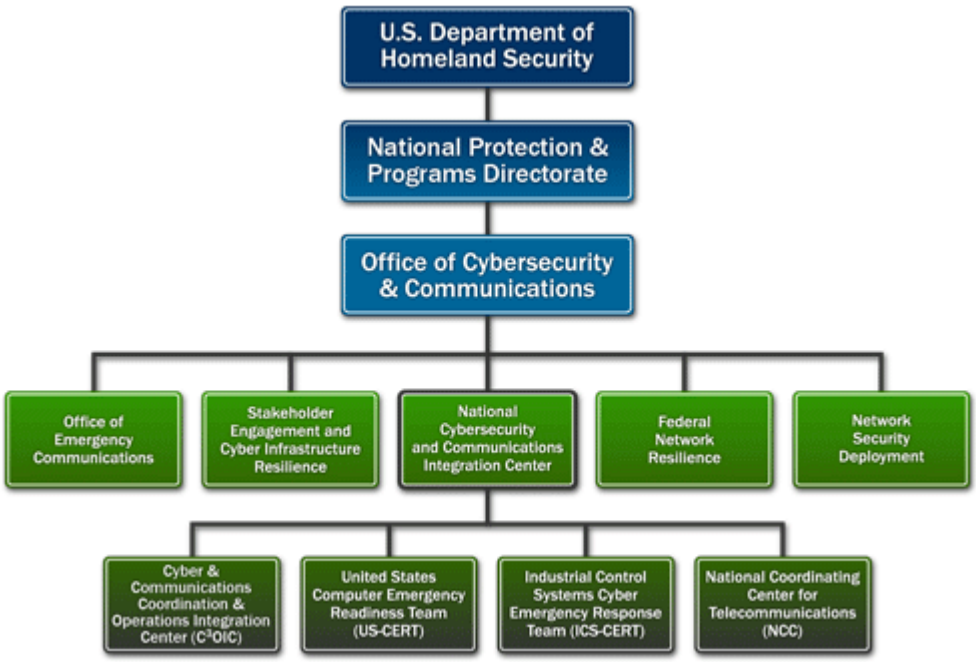
Different institutions could act as hosting organisations for teams charged with developing ICS-CERC. For capabilities aimed at the national level, n/g CERTs (or rather their host organisations) are just one of the options available. The well-established teams with ICS responsibility are usually parts of and/or funded by organisations with coordinating roles in national policies on CIIP (see below).

The baseline organisational needs of teams with ICS-CERC services might be similar to those of an existing CERT, including ensuring that they receive sufficient funding from the host organisation, have well-defined lines of responsibility and reporting, legal support, and determining whether they can use their host organisation's experience, expertise, and resources for their effective and efficient operation.

The teams that now exist at national level, that have ICS responsibility (for example ICS-CERT in the US) provide interesting insights into potential ways to position those teams. US ICS-CERT's host organisation for example is the National Cybersecurity and Communications Integration Center (NCCIC), which is under the auspices of the Office of Cybersecurity & Communications (CS&C), which is embedded within the Department of Homeland Security (DHS).

The organisational chart for the DHS, CS&C and NCCIC is shown below:

Figure 9: US DHS organisational chart[73]



[73] *Available at* http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

As another example in Japan ICS cyber-security is not separated out from the responsibilities of the n/g CERT. JP-CERT/CC operates its ICS-CERC services as an element of its 'traditional' duties. JPCERT/CC (almost fully funded by METI – Ministry of Economy, Trade and Industry)[74] supports its constituency with several types of ICS cyber-security services, including incident handling, ICS product vulnerability coordination, and awareness raising.

In Europe the current practice shows that ICS-CERC services have been developed either within the n/g CERT itself (Slovenia, Denmark) or within an organisation closely related to the n/g CERT activities (Portugal in academic and also de facto national CERT, Germany in Federal Office for Information Security, FORTH in Greece as a CERT). The host organisation characteristics regarded most positively by the teams with ICS responsibilities include:

- If the host organisation is not a regulator or military agency, it is easier for the teams to develop and maintain strong trust relationships with ICS vendors, industry sectors and other private sector organisations.
- It turns out that the best collaborative relationships are voluntary, not mandatory.
- It is an advantage to use reputation, experience, expertise, contacts and infrastructure of the host organisation in cyber-security and ICS.

CERT respondent: "We are a government institution that does not aim at making a profit – the industry partners appreciate this a lot."

[74] http://www.meti.go.jp/english/

2.4 How and why to develop good cooperative incident response capabilities for the ICS sector

2.4.1 Importance of cooperation

A cyber-incident impacting an industrial control system can have a significant negative impact not only on the organisation itself; it can also harm national security, cause injury or death of organisation employees or community members, damage equipment or the environment, or disrupt supply chains. ICS information infrastructure has become more interlinked in recent years, to an extent that ICS organisations themselves may not even be fully aware. This means that threats can rapidly cross boundaries between organisations and even nations.[75]

The attacks may be ***intentional and targeted*** like the well-known Stuxnet[76], a piece of malicious software detected in 2010, which focuses specifically on Siemens software and hardware, modifying the logics of Siemens S7 PLC microcontrollers and hiding this from the supervisory software application/ operators. ***Unintentional consequences or collateral damage*** from other attacks (not particularly targeted at the ICS) like worms, viruses or even simple ICS failures may, for example, cause havoc in railway and other transport flows.[77] But there are also ***unintentional incidents*** caused within ICS organisations while for example testing new software on operational systems or unauthorised changes to system configuration.[78]

This reality makes cooperation at any level crucial and indispensable for teams which have incident response responsibility over the ICS networks. The appointed team must serve as a single point of contact for all ICS organisations within its constituency. Further, this team should be a well-regarded incident responder and a trusted disseminator of important information. This makes developing trust with other similar teams and their constituencies very important, as well as cooperation between them and other (ICS) partners such as national bodies responsible for CIIP policies and ICS assets owners, provider and vendors. Trust is to be based on win-win aspects of collaboration, as for the constituents it is important to instigate collaboration as an open partnership, rather than to put in place a strict regulatory regime with sanctioning powers.

ICS respondent: "The high level of trust is crucial for effective incident handling."

[75] For more information on previous ENISA studies in the area of interdependencies see for example 'Cyber Security Aspects in the Maritime Sector' (https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts), 'Emergency Communications Stocktaking' (https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/emergency-communications-stocktaking), 'Good Practices for Resilient Internet Interconnections' (https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/resilience-of-interconnections) or the already mentioned 'Protection of ICS: Recommendations for Europe and Member States' (https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems)

[76] Falliere, Nicolas, Murchu, Liam O and Chien, Eric. W32.Stuxnet Dossier. Symantec. 2011

[77] Tsang, Rose. Cyberthreats, Vulnerabilities and Attacks on SCADA networks. 2009.

[78] As a result a power plant may be shut down for longer periods, a plane may crash or a satellite may be misplaced. See the article 'The Role of Software in Recent Catastrophic Accidents' in the IEEE Reliability Society Annual Technology Report 2009 (http://paris.utdallas.edu/IEEE-RS-ATR/document/2009/2009-17.pdf).

The importance of cooperation at both a domestic and international level must be recognised and implemented at an early stage when building the capabilities. In ideal circumstances, the cooperation links should be well defined and workable with CIIP policy bodies, law enforcement agencies and the intelligence community to coordinate incident response efforts among federal, regional and local governments, when necessary.

However, the priority is to establish and maintain collaborative relations with all ICS, assets owners and vendors concerning providers within the constituency according to the service portfolio. In addition, cooperation needs to be extended to other CERTs in order to share ICS-related security incidents and mitigation measures.[79]

Including all these stakeholders will contribute to strengthening the resilience of national critical (information) infrastructures, and thus national security, and to mitigating the impact of the ICS incidents based on the lessons learned. Broader exchange of best practices among the teams with ICS responsibility is necessary to improve the incident response capabilities of these systems in the future.

2.4.2 Choosing partners for cooperation at the national level

The underlying objective and focus for teams with ICS responsibility must be to protect critical information infrastructure and support the seamless functioning of ICS that are indispensable for this infrastructure. It is of utmost importance to understand the difference in approaches to solving incidents in traditional ICT systems and those affecting ICS (as laid out in this report). While for ICT systems confidentiality and integrity might be the main concern, for ICS these factors pertain to human safety, environmental impacts and the process itself (loss of equipment/ production). Therefore; availability ranks highest among the three fundamental characteristics of cyber-security in this area. This aspect needs to be reflected in cooperation between teams with ICS-CERC and relevant stakeholders.

The cooperation activities will often involve many actors, including governmental bodies, law enforcement agencies (LEA), CERTs in the country, and mostly private sector companies dealing with ICS. The cooperation with national CIIP authorities must be formally established and based on national CIIP strategies and regulations. With private or semi-private ICS constituents the cooperation is generally voluntary, which makes it important for the team to demonstrate trustworthiness, reliability and operational incident response capabilities.

ICS asset owners and services providers

Cooperation and communication with ICS providers and asset owners is also crucial. Unfortunately, lack of knowledge about a team's existence or its capabilities can make it more challenging for the team to benefit from cooperative efforts at a domestic level with these partners. So, the first task (much more important than in the case of other cooperative partners) is to promote awareness of their own existence and their value proposition for the constituents.

The informal nature of cooperation and maintaining trust-based personal contacts is advisable, again more so than in the case of other cooperative partners, based on the observed practice for effective service delivery and a fruitful bilateral collaboration. This relates especially to on-site visits of ICS-CERC team’s personnel to ICS asset owners’ facilities (like transport control systems in railway or air traffic, power plants, dams, chemical factories, food processing) in order for the technical personnel to get acquainted with specific features of ICS in the constituency. Staff who maintains the systems

[79] See Control Systems Security Program, ICS-CERT, available at http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_ICSCERT-FactSheet-v8.pdf

(e.g. system administrators, PLC operators) should be educated in the more general issues of cyber-security and incident handling.

One challenge that is likely to arise is to establish a good operational incident reporting mechanism with the ICS providers. In the short term, it will not be easy to mandate such cooperation because of a general skepticism, lack of knowledge or trust in the team's discreetness. The outlined cooperative approach which is based more or less on a voluntary model (after the industry players become aware of the ICS-CERC's existence and especially its usefulness) is probably the best way to start. In the longer term, teams with ICS-CERC should work with the national policymakers and ICS asset owners and providers to discuss whether mandatory incident reporting could improve the practice and bring any additional value to the operations.

ICS vendors

Cooperation and timely information sharing with ICS vendors is also very important. ICS vendors face their own challenges in terms of convincing their customers of the importance of ICS cyber-security, and have to be realistic in that their customers' interest levels in ICS cyber-security matters can depend primarily on whether they have already been impacted by a cyber-security incident or not.

ICS vendors must focus on ensuring the security of their products and services, and it is important that teams with ICS-CERC services understand how vendors are trying to accomplish this to improve their cooperation and lines of communication. Vendors can do this in a number of ways, but broadly speaking, they will try to:

- Integrate security features into their devices and then help their customers maintain security through service-level agreements (SLA);
- Implement security standards (e.g. ISA/IEC-62443, formerly ISA 99)[80] and compliance requirements (e.g. North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP) compliance requirements);
- Provide best practices to their customers on how to implement security features to their products;
- Provide follow-up services to their customers, including patches and vulnerability announcements.[81]

To the extent that teams with ICS-CERC capabilities can form positive relationships with vendors, this can be beneficial to their efforts to offer quality and timely ICS services (like alerts and warnings) to their constituency.

N/g CERTs and other CERTs

The relationship with the n/g CERT in its country is especially important – especially where ICS-CERC services should be provided at a national level. Their activities must generally be coherent and streamlined (complementary to each other if feasible), for example in the case of coordination of incident management processes. It is up to the Member States to decide whether teams with ICS responsibility should be separate entities, divisions of existing n/g CERTs or work under any other arrangements. But as n/g CERTs are regarded as a single point of contact for other CERTs within the boundaries of their countries and globally, it is desirable that ICS-CERC teams also join the CERT communities. Via these platforms they will be in a better position to exchange information on 'general' ICT incidents and ICS in particular as some industrial CERTs may also take part in the activities of these platforms.

[80] http://www.isa.org/autowest/pdf/Industrial-Networking-and-Security/Phinneydone.pdf.
[81] Analysis based on interviews with vendors conducted in conjunction with this study.

CERT respondent: "The implementation method and placement of countermeasures or defences may be different [for ICS-CERC teams], and the business domain may also impose different or stricter requirements towards reliability and availability."

National bodies responsible for CIIP agenda

As ICS in sectors like energy, water treatment, transport, chemicals and others constitute a part of critical infrastructure, it is a necessity that the team responsible for ICS area establishes and maintains a good relationship and cooperation with all relevant bodies responsible for CIIP at national level. This cooperation can be defined in national CIIP strategies and regulations. The criticality of ICS requires that such cooperation can be activated as fast as possible after a serious incident affecting ICS, and therefore critical infrastructure, is detected. Possible arrangements for the cooperation could take a form of a cyber-security council or national crisis committee. The teams with ICS-CERC will probably not have the main decision-making role, but should have an advisory role, because of the incident response expertise.

Law enforcement agencies

Cooperation with law enforcement agencies (LEA) is another key domestic relationship. As the attacks on critical infrastructure can have criminal aspects (sabotage, act of terrorism or other hostile political motives), the police and the judiciary also need to be involved. It is necessary to bear in mind that the information flow will probably be mostly unidirectional – from the team to LEAs as is documented by current practice.[82] On the other hand, the team should regard this cooperation as one of its crucial partnerships due to the possible impact of ICS incidents, so the team should be a valuable source of information and expertise for LEAs. For example, the above-mentioned Stuxnet can be considered as a reference model, a step-by-step guideline for a future generation of malware against ICS.

2.4.3 Cooperation at cross-border level

ICS cyber-security and threats raise specific issues touching on sensitive matters such as national security that are less common with traditional ICT cyber-attacks. This makes information sharing harder to achieve, especially across borders, and will in turn place a significant benefit to trust. It needs to be said that with the interlinking of ICS across borders the complexity of cooperation and especially legal implications increases.

Cyber-attacks on industrial control systems may easily occur across national borders and impact organisations with operations in many different countries. The attacks include massive distributed denial of service attacks (DDoS), efforts to penetrate networks undetected, DNS poisoning, SQL injection attacks or malware infections. The aims of the attacks vary from shutting down services or operations to the theft of services and data or extortion attempts. According to a study 'In the Crossfire: Critical Infrastructure in the Age of Cyber War' conducted by McAfee,[83] the most sensitive

[82] See ENISA's report on information sharing between CERTs and law enforcement agencies at http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/supporting-fight-against-cybercrime/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices/at_download/fullReport

[83] http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf

critical infrastructures in energy and natural-resource industries (such as water and sewage plants), are some of the least secure. Executives at water and sewage facilities also reported having the lowest level of security measures in place.[84] Especially when these facilities are located close to national borders (for example dams and water reservoirs), incidents affecting their control systems may have serious repercussions for critical infrastructures in more Member States. However, the immediate geographic distance is of less importance when it comes to attacks and disruptions relating to power plants or transport flows.

Thus, incident responses may need to be coordinated across countries or synchronised between ICS and other actors in a number of different countries. Further, best practices for responding to and preventing attacks on industrial control systems become less and less country-specific. These factors favor cooperation at the cross-border level, as is also necessary when dealing with large-scale cross-border ICT incidents.

This cooperation can create efficiencies in facilitating response for teams with ICS responsibility, for example as regards mitigation of incident impacts that sever energy supplies and cross-border high-speed railway transport. Resources of the teams providing ICS-CERC services could be limited, and capabilities need to be built up to face challenges resulting from the attacks on ICS. This means that best practices need to be taken note of and used, and ICS knowledge should be built as efficiently as possible. Knowledge sharing with other existing and experienced teams and industry players is one relatively straightforward way to accomplish this.

On an international level, there are a number of challenges to cooperation on ICS cyber-security matters. Teams with ICS responsibility are not as widespread or as well-known as traditional CERTs, so there is not a robust network of similar players or a wide European community in place as teams develop their ICS-CERC. However, as pointed out earlier in this document, utilising the expertise and experience of existing CERT communities would be beneficial for a team charged with ICS-CERC services.

A number of organisations offer international forums or facilitate cooperation among ICS players.[85] Organisations that focus on ICS security matters such as CIGRE or even broader CERT community organisations such as FIRST and industry associations can be useful resources, and could be important to the development of operational and effective incident response cooperation at an international level.

A respondent from the ICS sector noted very good cooperation within NAMUR, an international user association in the chemical and pharmaceutical processing industries, where information is shared among attendees.

Another respondent noted that his team is a member of FIRST and that its customers were willing to discuss ICS-related matters with it in this forum.

[84] Ibid.
[85] For more information see 2.1.5 and footnote 36.

CERTs with an ICS-CERC agenda are not always members of EuroSCSiE or any other European and global initiative dealing with ICS and its cyber-security aspects. Teams to be tasked with ICS-CERC services could welcome such discussions and forums and should take an active part in them. Thus, participating in international ICS forums and developing relationships with other teams could be a fundamental part of efforts by teams with ICS-CERC to develop and to better serve their constituents. Besides, it is recommended that such teams seek recognition among the wider CERT community. Membership to or accreditation at FIRST or Trusted Introducer,[86] although not specifically focused on ICS, can be a very good step to gaining recognition and acceptance by experts in the area of incident response capabilities. Some of the industry players are already engaged in these organisations and initiatives via their incident response teams.

At the same time, it is logical to establish mutually beneficial bilateral relations with teams in other countries. Some of the teams that can be seen as demonstrating good practices in ICS-CERC in Europe and beyond have been mentioned in this document. Other examples will inevitably follow as more teams with ICS-CERC are established and attain a certain degree of maturity.

[86] https://www.trusted-introducer.org/index.html

3 Conclusions

This document provided an overview of many of the important considerations for a team charged with developing ICS-CERC services, with a special view on incident management capabilities. As stressed throughout the document, there are some unique challenges associated with providing cyber-security services for industrial control systems, but the process can be made more manageable by following **identified good practices for CERTs** and taking into account experiences which exist already in Europe and globally. Information sharing and cooperative efforts are indispensable elements of the development efforts.

The responsible team needs to bear one paradigm in mind, which is different for ICS compared to traditional ICT systems. It is the priority aspect on the three-stranded CIA security scale: confidentiality, integrity, availability. While for traditional ICT systems the main priority is integrity, for ICS **availability** ranks highest. This has a lot to do with the fact that ICS are indispensable for the seamless operation of critical infrastructure. Cyber-incidents affecting ICS can have disastrous effects on country's economy and people's lives. They can cause long power outages, paralyse transport nationally and internationally and cause ecological catastrophes. In order to face these challenges, it is of utmost importance that the team is equipped with all the capabilities of a 'typical' well-functioning CERT but with additional adjustments for the ICS environment.

As protection of critical infrastructure (and thus of ICS) is a matter of national interest, often embedded in national CIIP strategies and regulations, there should be a **clear mandate** defined, especially for incident management activities. The main constituents will be large ICS players (energy companies, transport companies, chemical industry, food processing), which, unlike constituents of traditional CERTs, sometimes do not have sufficient expertise in cyber-security. On the other hand, the established CERTs do not necessarily understand or have a deeper knowledge of sector-specific technical aspects of ICS.

Incident handling is a core service that every CERT must provide, and should also be considered a core service in the ICS area. Incident handling service in the ICS context will be challenging to develop, as a result of (for example) the type and priority of incidents, different standards and procedures to deal with and manage, the type and size of the network and (national, regional or global) distributed network nodes (ICS objects). An initial challenge for teams responsible for providing incident handling service is to get information about an ongoing cyber-incident impacting an industrial control system. There is usually no legal duty for private ICS asset owners, vendors, or network service providers to report incidents, and these players may not be comfortable sharing this information. This makes it important that a team **demonstrates trustworthiness and transparency** and builds confidence in its abilities to handle data and information with complete confidentiality.

The **hiring process** for staff on teams responsible for developing ICS-CERC services is an important matter that should be given sufficient consideration. In particular, the process should acknowledge the fact that staff will be dealing with CII matters and helping ICS players handle incidents that have the potential to cause significant damage. This means that staff should be vetted thoroughly in the recruitment process, and consideration should be given to factors such as an individual's ability to perform under pressure and willingness to be on-call for incident handling and response at non-working hours. This is important not only for the development of ICS-CERC services in a team, but also for making sure that ICS vendors, industry players, and even governmental agencies are comfortable working with the team as it establishes its services.

The importance of **cooperation at both the domestic and international level** must be recognised and implemented when building the incident response capabilities. In ideal circumstances, the team partners with CIIP policy bodies, law enforcement agencies and the intelligence community,

coordinates incident response efforts among federal, regional or local involved partners, and works with ICS asset owners, operators, and vendors on regular basis. Additionally, teams should collaborate with other ICS players and CERTs to share ICS-related security incidents and mitigation measures. Including all these stakeholders will contribute to strengthening the resilience of national critical (information) infrastructures, and thus national security, and to mitigating the impact of the ICS incidents. **Broad exchange of good practices** among teams with ICS responsibility is necessary for improving incident response capabilities in the future.

Next steps

This document needs to be considered as an initial attempt to provide a good practice guide for the teams to be tasked with incident response capability for industrial control systems. For this reason it is a living document that will be periodically updated in line with the evolving cyber-security landscape and, of course, also in line with experiences of the EU Member States in deploying this capability in their respective countries. In addition to existing activities in ICS such as providing CERT training material, ENISA is ready to facilitate the exchange of the good practices via aggregate reports, analysis and CERT workshops. ENISA also welcomes and encourages any suggestions of ICS stakeholders from the public, private and non-profit sectors with the objective to improve and update this guide.

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu