D5.2 – Cybersecurity guidelines

Renewable and Waste Heat Recovery for Competitive District Heating and Cooling Networks

REWARDHeat

Project Title: Renewable and Waste Heat Recovery for Competitive District Heating and Cooling Networks

Project Acronym: REWARDHeat

Deliverable Title: Cybersecurity guidelines

Lead beneficiary: RINA-C

Federica Fuligni, RINA-C

Giampiero Savina, RINA-C

Ahmad Karim, ENISYST

Simone Buffa, EURAC Research

Due date: 30 September 2020

QUALITY CONTROL ASSESSMENT SHEET			
Issue	Date	Comment	Author
V0.1	06.02.2020	First draft sent to reviewers	Federica Fuligni
V0.2	17.04.2020	Second draft sent to reviewers	Federica Fuligni, Simone Buffa, Ahmad Karim
V0.4	22.05.2020	Third draft sent to reviewers	Federica Fuligni, Giampiero Savina
V0.5	23.09.2020	Final draft sent to reviewers	Federica Fuligni, Giampiero Savina
V0.6	25.09.2020	Final review	Simone Buffa
V1.0	30.09.2020	Submission to the EC	Roberto Fedrizzi

This document has been produced in the context of the REWARDHeat Project.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 857811. The European Commission has no liability for any use that may be made of the information it contains

Table of Contents

1 Introduction

Cyberattacks are malicious attempts to damage, steal or destroy critical corporate data, compromise websites, and disrupt operational infrastructures. These attacks are usually perpetrated through the electric and electronic network, which are also present in common district heating and cooling (DHC) infrastructures, as the ones in the REWARDHeat project.

This document has the aim of guiding DHC operators to implement cyber-security strategies in the SCADA system of their systems or for proprietary SCADA software in order to provide resilient and secure services for the DHC market.

The report presents cyber-security strategies and guidelines that should be foreseen in modern DHC networks according to the legislative framework, with a focus on the necessary protections to avoid disruptions that could cause critical damage to the DHC system.

A methodology for the assessment of the cybersecurity risk and possible threats (both cyber and physical accidents) for DHC systems is proposed and applied to two reference DHC netowrk systems.

Supervisory control and data acquisition (SCADA) systems for an existent or new district heating and cooling (DHC) network are also described.

Finally, guidelines to mitigate cybersecurity attacks in DHC networks SCADA systems are suggested.

2 Cybersecurity and privacy management requirements for DHC networks

2.1 Introduction to relevant legislation

The costs of cybercrime for businesses are increasing, especially since the EU legislation on the General Data Protection Reform (GDPR) and the lockdown in the early months of 2020 have moved operations almost completely online.

We have analysed different sources for cybersecurity in the energy sector, from the industrial and research perspective. The most relevant publications are:

- "Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector", Energy Expert Cyber Security Platform (EECSP)[1], February 2017 , and
- "Cybersecurity of critical energy infrastructure", European Parliamentary Research Service (EPRS), October 2019.

The main international regulation on the matter are of critical infrastructure is:

- ISO/IEC 27001:2013 (incl. Cor.1:2014 & Cor. 2:2015)

For the purpose of this deliverable, a reference to the German industry security standard for district heating has also been consulted, as it contains guidelines on the definition and implementation of security measures in district heating, which are also applicable to other EU countries:

- Industry specific security standard for the distribution of district heating (AGFW 2018), original: *Branchenspezifischer Sicherheitsstandard für die Verteilung von Fernwärme (B3S VvFw*), AGFW and BDEW, 2018.

German National Strategy for Critical Infrastructure Protection (CIP Strategy) and Cyber Security Strategy have finally been consulted[2].

2.2 Critical infrastructure in DHC networks

District heating distribution refers to the supply of heat across property boundaries. District heating is distributed in the form of hot water or steam. The district heating water flows in a circulatory system from the heat generation plants (heating power plants and heating plants) to the customer and back. District heating networks can be organised in five main assemblies:

[1] The mission of the EECSP-Expert Group is to provide guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies and nuclear.

[2] https://www.kritis.bund.de/SubSites/Kritis/EN/strategy/strategy_node.html

1. **the actual pipeline network**, consisting of a feed for the distribution of the hot district heating water and a return of the cooled district heating water. In the case of a two-wire network, there is a single feed for space heating and hot water preparation, as well as a single return pipeline. Three-wire networks have usually two supply lines, one for the space heating and one as a constant heat conductor for the in-house water heating;
2. **the pumping stations**, used for overcoming the pressure losses in the district heating network and thus for the transport of district heating water quantities;
3. **the control room for the main control**, responsible for monitoring and, if necessary, controlling the district heating supply. The control usually reacts to signals of a pressure measurement or difference. In the event of a load change in district heating, the flow rate of the pumping stations can be adjusted via the remote-control technology or by manual intervention. One of the main tasks is to ensure an economically optimal driving style of the district heating network as well as the feed-in from the generation plants;
4. **the central control technology** supports the management staff in their tasks. It is generally an interface for monitoring the district heating network. It is used to improve district heating network conditions, load forecasts, timetables, etc. For example, it adjusts speed changes at the pumps. The signals are transmitted by means of telecontrol technology, e.g. to the programmable logic controller (PLC) of the pumps. Fault messages from the district heating network are also displayed and can be efficiently processed;
5. **the transfer station** (technical equipment) is the link between the pipeline network and the customer's headquarters. It usually falls within the area of responsibility and physical space of the customer. It is used to determine the heat as intended, e.g. in terms of pressure, temperature and volume flow, to the house headquarters.

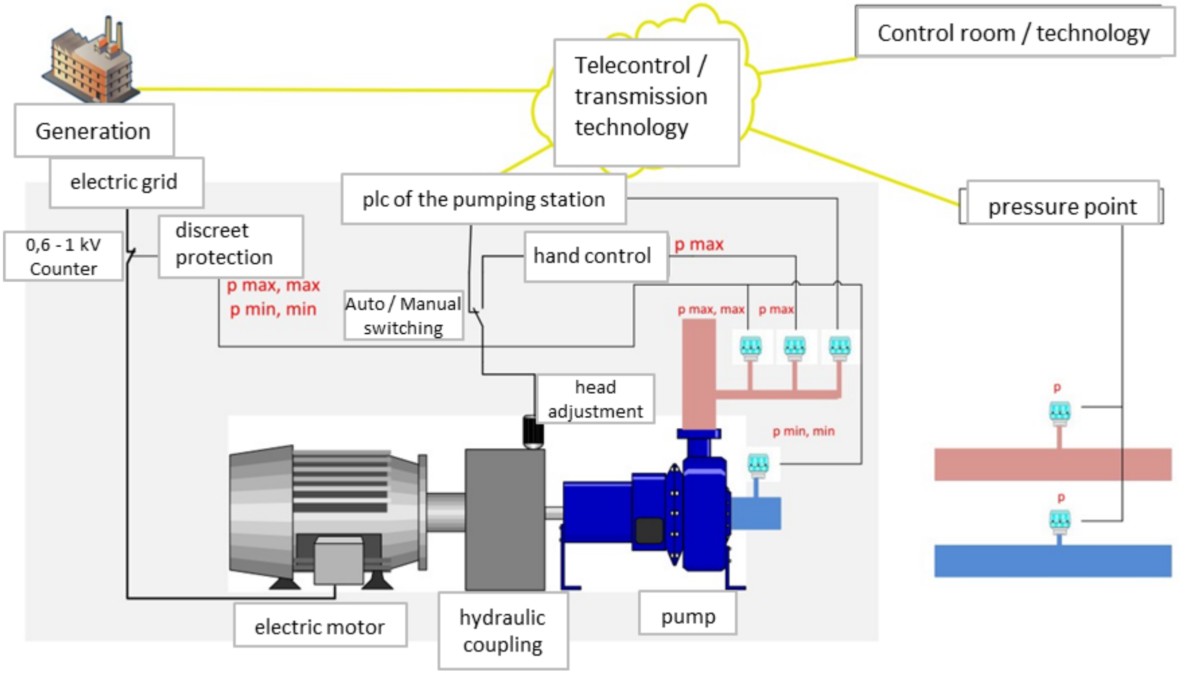

Figure 1: Equipment considered as part of the critical infrastructure according to the German standard. Translated from (AGFW 2018).

It is outside the scope of the security standard for the distribution of district heating (AGFW 2018):

- The customer's equipment, where we can find:
  - the transfer station,
  - the house system, consisting of the piping system from the house headquarters, the heating surfaces and the associated shut-off, control and control devices.
- The generation plants for the supply of heat, e.g. combined heat and power plants,
- The pipeline network, if the present IT equipment doesn't have an impact on the operation of the critical infrastructure.

3 Methodology for cybersecurity risk evaluation in DHC systems

3.1 Methodology

In this section, a methodology for performing a risk analysis is proposed and the cybersecurity risk is assessed for a reference DHC system. Generally speaking, the risk analysis is the process of identifying vulnerabilities and threats to the resources used by an organization in achieving objectives, and deciding what countermeasures are necessary to reduce the risk to an acceptable level.

In the framework of REWARDHeat, this activity is performed at the DHC system level and is the key for defining measures for the thermal grid, plants and substations maintenance, security and early fault detection in order to increase the system resilience.

From a methodological point of view, the risk analysis in REWARDHeat has been carried out following this approach:

1. identification of sensitive objects;
2. evaluation of the sensitive objects in terms of confidentiality, integrity and availability;
3. identification of applicable threats ;
4. evaluation of the sensitive objects in terms of impact and probability;
5. evaluation of risk.

3.2 Identification of sensitive objects

The sensitive objects are the parts of a subsystem that manage the identified sensitive data or/and signals that are important from the functional/operational point of view of the DHC system. The subsystem may be defined also with the help of the current legislation or standards (as for the German case).

3.3 Evaluation of the sensitive objects in terms of confidentiality, integrity and availability

There is a need for protection for information technology systems, components or processes when these are decisive for the operation of the critical infrastructure. The following methodology partially comes from the protection objectives from KRITIS[3] and other national (e.g. Italian) standards.

In particular, we have identified that the sensitive objects shall be quoted in terms of *confidentiality*, *integrity* and *availability* of the data or/and signals, as explained below:

- **availability**: means that with a digital control of the district heating pumps, the IT systems and remote control techniques used for this purpose are available, i.e. functional;
- **integrity**: means that digital control impulses emanating from the IT system arrive and are implemented in the control room in an unadulterated manner, as well as digital impulses of the control room arrive and are implemented in the IT system in an unadulterated manner;

[3] https://www.kritis.bund.de/SubSites/Kritis/EN/strategy/strategy_node.html

- **confidentiality**: includes protection against the unauthorized release of information and data from IT systems to third parties.

The objective of *authenticity* was also included in the German standard (AGFW 2018), but for the sake of our investigation we assume that data is reliable and verifiable, and thus this objective is always met.

To each of these terms, we will then associate a level and a weight factor, leading to a final quantitative result of the quotation process presented in the following sections. The weighting factors are described in the following tables.

Once defined the quote for each term, it is possible to calculate the *average quote for the object* according to equation 1:

$$Q_{Obj} = \frac{Q_{Availability}+Q_{Integrity}+Q_{Confidentiality}}{3} \qquad [1]$$

Table 1 – Level of data or/and signals availability.

Level of availability	Description	Weight
Maximum (M)	The object impacts severely and directly on the availability of data or/and signals and may compromise their purpose.	1
High (H)	The object impacts significantly on the availability of the data or/and signals but without irrecoverable consequences.	2/3
Normal (N)	The object impacts on the availability of the data or/and signals but without important consequences.	1/3
Without (W)	The object does not impact the availability of the data or/and signals.	0

Table 2 – Level of data or/and signals integrity.

Level of integrity	Description	Weight
Maximum (M)	The object impacts severely and directly on the loss of integrity of the data or/and signals and may compromise their purpose.	1
High (H)	The object impacts significantly on the loss of integrity of the data or/and signals but without irrecoverable consequences.	2/3
Normal (N)	The object impacts the loss of integrity of the data or/and signals but without important consequences.	1/3
Without (W)	The object does not impact on loss of integrity of the data or/and signals.	0

Table 3 – Level of data or/and signals confidentiality.

Level of confidentiality	Description	Weight
Highly Critical (HC)	The asset is highly critical for the overall functioning and integrity of the system. If disrupted the overall system could enter a critical status. Damages and harms that occurred upon disruption could be serious for the overall system. The service level agreement (SLA) terms and conditions will not be met and even the restoration of the system would take a considerable amount of time and resources. Moreover, the asset manages information that, if disclosed, would provide the attacker with highly critical and sensitive information about the overall system and its services.	1
Critical (C)	The asset is critical for the functioning of the system. If disrupted the service level agreement (SLA) terms and conditions would not be respected, causing a big degrade in performance and image, as well as financial, damage. The asset manages critical information that if disclosed could provide the attacker critical information about the system configuration services and functions.	2/3
Relevant (R)	The asset is relevant for the functioning of the system within the service level agreement (SLA) terms and conditions. A disruption of the asset would cause a degrade in performance which still is acceptable, but it should be managed. Moreover, the asset manages information that could provide relevant information about the system architecture or system functions.	1/3
Not Relevant (NR)	The asset is not relevant to guarantee that the system is unharmed, and its replacement/repairing time is well below the service level agreement (SLA) terms. Moreover, the asset is not relevant from the information point of view.	0

3.4 Identification of applicable threats

The *applicable threats* have been identified by RINA, with the support of EURAC. They are comparable to those reported in the German standard (AGFW 2018). They have been divided into two groups: the threads related to cybersecurity accidents, and the threads related to physical accidents as summarised in Table 4 and Table 5 respectively.

The threads related to cybersecurity mainly concerns: damage and loss of IT assets (e.g. damage by third party, loss of sensitive information and digital documents and records), unintentional data damage (e.g. data alteration or information leakage due to user error, inadequate design, planning and adaptation), failures and malfunction (e.g. failures of services or communication links, disruption of main supply functions, malfunction of devices) and nefarious activity, abuse (e.g. software management, access to the network, malicious code, unauthorised access to systems or Compromising confidential information).

For what regards the threads related to physical accidents it has been considered: natural disasters (e.g. fire, thunder-stroke), deliberate physical attacks (e.g. bomb attack, sabotage, vandalism and theft), loss or failure of IT assets (hardware) and outages (physical damage to the network due to testing, loss of supporting device, strike, shortage of personnel and energy outage).

Table 4 – Threads related to cybersecurity.

Damage, loss of IT assets - software				
Damage by third party (on the software)	Loss of Sensitive Information	Loss of media, digital documents	Destruction of digital records (e.g. database)	Information leakage
Unintentional data damage				
Information leakage due to user error (e.g. use weak passwords)	Erroneous use or administration of devices and systems	Using information from unreliable source	Unintentional data alteration	Inadequate design, planning, adaptation
Failures and malfunction				
Failures of services (e.g. malfunctioning due to lack of veriication)	Failure, disruption of communication links (e.g. an application is not working as is should)	Failure, disruption of main supply functions (e.g. switch of devices through remote action)	Failure, disruption of service providers (e.g. bank system not working, concerns non proprietary systems)	Malfunction of devices, systems
Nefarious activity, abuse (software management, access to the network)				
Denial of service	Malicious code, malicious activity	Abuse of Information Leakage	Manipulation of HW and SW	Manipulation of information
Misuse of information, information systems	Unauthorised use of administration	Unauthorised access to systems	Unauthorised software installation	Unauthorised use of software
Compromising confidential information	Abuse of authorizations	Remote activity (execution)	Targeted attacks	

Table 5 – Threads related to physical accidents.

Natural disasters				
Natural or environmental disaster	Fire	Thunder-stroke		
Deliberate physical attacks				
Bomb Attack	Sabotage	Vandalism	Theft	
Loss or failure of IT assets (hardware)				
Loss of devices (e.g. sticker, monitor	Failures of devices (e.g. ruined CD			
Outages (physical damage to the network)				
Damage from testing	Internet outage	Network outage	Loss of support devices	Strike
Shortage of personnel	Lack of resources	Energy outage	Shortage of personnel	Lack of resources

3.5 Evaluation of the sensitive objects in terms of probability and impact

The sensitive objects are also to be calculated against:

- the occurrence probability evaluated as with extremely high, high, low or null according to the weights listed in Table 6;
- the impact of the threat on the sensitive objects, in terms of confidentiality, integrity and availability, evaluated as with extremely high, high, low or null according to Table 7.

Table 6 – Weight factor (0_i) used for the occurrence probability evaluation.

Extremely high (EH)	Threat should occur with an extremely high (EH) occurrence probability.	1
High (H)	Threat should occur with a high (H) occurrence probability.	0.92
Low (L)	Threat should occur with a low (L) occurrence probability.	0.74
Nil (N)	Impossible to realize in practice.	0

Table 7 can be considered as an example and the final values are subject to the assessor decision and reasoning. It is provided as a guideline to determine which value best fits the impact, according to the values provided to availability, integrity and criticality.

Table 7 – Weight factor (I_i) used for the impact evaluation of the threat.

Impact	Availability	Integrity	Confidentiality	Weight I_i
Extremely High (EH)	Maximum	Maximum	Highly Critical	1
High (H)	High	High	Critical	0.92
Low (L)	Normal	Normal	Relevant	0.74
Nil (N)	Without	Without	Not Relevant	0

Each sensitive object has to be evaluated considering the product (P_i) -see

Table 8 -of the weight for the occurrence probability (O_i) of the i-th threat and the weight for the impact (I_i) on the *sensitive object*. The global occurrence/impact factor for each *sensitive object* (I_{Obj}) is obtained buy summing all the products of the occurrence probability and impact weights for each i-th threat and dividing it by the total number of threats N according to equation 2:

$$I_{Obj} = \frac{\sum_{i=1}^{N}(O_i \cdot I_i)}{N} = \frac{\sum_{i=1}^{N} P_i}{N} \qquad [2]$$

Table 8 – Occurrence / Impact weighting product result (P_i).

O/I reference value	N	L	H	EH
N	0.00	0.00	0.00	0.00
L	0.00	0.55	0.68	0.74
H	0.00	0.68	0.85	0.92
EH	0.00	0.74	0.92	1.00

Finally, the risk evaluation for the object (R_{Obj}) is calculated as the product of the quote (Q_{Obj}) and the global occurrence/impact factor (I_{Obj}) for each *sensitive object* divided by 2 according to equation 3:

$$R_{Obj} = Q_{Obj} * I_{Obj} \qquad [3]$$

At the end of this phase, every *sensitive object* (asset) is associated to a risk value. As an example in Table 9, red cells indicate a high risk, while yellow cells indicate a medium risk and green cells indicate a low risk.

Table 9 – Example of Asset and associated Quote, O/I and Risk Value assessment.

Asset	Quote value(Q_{Obj})	Occurrence / Impact factor (I_{Obj})	Risk (R)
Asset n1	0,22	0,32	0,07
Asset n2	0,56	0,46	0,26
Asset n3	0,67	0,46	0,31

4 Risk assessment for two reference DHC networks

The information collected in this chapter comes from an interview performed with two DH operators that are partners of the REWARDHeat project. The methodology presented above for the risk analysis has been implemented in an excel tool that has been used to assess and compare the risk of physical incidents and cyberattacks.

4.1 DH network – 1

The sensitive objects have been selected following the national legislation on the matter and comprise a control room and the pumping station(s). The results of the analysis are summarised in Table 10 whereas the main outcomes are:

- when quoting the sensitive objects, the control room shows the highest relevance, with the highest rate attributed to the integrity of the control;
- for what concerns the cyber-threats, both the control room as well as the pumping station show a medium to high impact/probability risk. The cyber-threats with the highest impact/probability risk are: the damage by third party, the failure or disruption of communication links and of main supply functions in the control room, and failure or disruption of communication links in the pumping station;
- the pumping station shows a higher impact/probability risk for physical accidents with respect to the control room. In particular, the worst regarded accidents in both objects are fire, bomb attack, sabotage, vandalism, network outage and energy outage;
- the combination of quoting and impact/probability shows that the control room is more exposed and susceptible to both cyber and physical attacks than the pumping station.

Table 10 - Risk analysis results for the reference DH network -1

Asset/sensitive object	Quote value(Q_{Obj})	Occurrence / Impact factor (I_{Obj}) - Cybersecurity	Occurrence / Impact factor (I_{Obj}) - Physical accidents	Risk for cyber attacks	Risk for physical accidents
Control room	0.78	0.69	0.68	0,54	0,53
Pumping station	0.44	0.69	0.71	0,30	0,31

4.2 DH network – 2

The sensitive objects have been selected following the national legislation on the matter and comprise a control room, substations at the building level and the pumping station(s). The results of the analysis are summarised in Table 11 whereas the main outcomes are:

- when quoting the sensitive objects, the control room and the pumping station show the highest relevance;
- for what concerns the cyber-threats, the control room shows a medium impact/probability risk. The cyber-threats with the highest impact/probability risk at the control room are: the

damage by third party, the failure or disruption of communication links and of main supply functions;

- the pumping station and the control room show a higher impact/probability risk to the physical accidents. In particular, the worst regarded accidents in both objects are natural or environmental disasters, fire, bomb attack, sabotage, vandalism, theft;
- the combination of quoting and impact/probability shows that the control room is more exposed and susceptible to both cyber and physical attacks, while the pumping station also presents a medium risk to physical accidents. Concerning the substations at the building level, the risk for physical accidents is higher than the one for cyber attacks.

Table 11 - Risk analysis results for the reference DH network -2

Asset/sensitive object	Quote value(Q_{Obj})	Occurrence / Impact factor (I_{Obj}) - Cybersecurity	Occurrence / Impact factor (I_{Obj}) - Physical accidents	Risk for cyber attacks	Risk for physical accidents
Control room	0,56	0,55	0,63	0,31	0,35
Pumping station	0.44	0.69	0.71	0,06	0,13
Substations at building level	0,44	0,13	0,29	0,10	0,36

5 Description of a SCADA system for DHC systems

A legacy supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications and graphical user interfaces (GUI) for high-level process supervisory management, while also comprising other peripheral devices like programmable logic controllers (PLCs) and discrete proportional-integral-derivative (PID) controllers to interface with process plant or machinery.

5.1 SCADA System components

SCADA system usually consists of the elements described in the following sections.

5.1.1 Supervisory computers

This is the core of the supervisory control and data acquisition (SCADA) system, gathering data on the process and sending control commands to the field connected devices. It refers to the computer and software responsible for communicating with the field connection controllers, which are remote terminal units (RTUs) and PLCs, and includes the human-machine interface (HMI) software running on operator workstations. In smaller SCADA systems, the supervisory computer may be composed of a single PC, in which case the HMI is a part of this computer. In larger SCADA systems, the master station may include several HMIs hosted on client computers, multiple servers for data acquisition, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual-redundant or hot-standby formation providing continuous control and monitoring in the event of a server malfunction or breakdown.

5.1.2 Remote terminal units

Remote terminal units, also known as (RTUs), connect to sensors and actuators in the process and are networked to the supervisory computer system. RTUs have embedded control capabilities and often conform to the IEC 61131-3 standard (IEC 2013) for programming and support automation via ladder logic, a function block diagram or a variety of other languages.

5.1.3 Programmable logic controllers

Also known as PLCs, these are connected to sensors and actuators in the process and are networked to the supervisory system. In factory automation, PLCs typically have a high-speed connection to the SCADA system. In remote applications, such as a large water treatment plant, PLCs may connect directly to SCADA over a wireless link, or more commonly, utilize a remote terminal unit (RTU) for the communications management.

5.1.4 Communication infrastructure

This connects the supervisory computer system to the RTUs and PLCs and may use industry standard or manufacturer proprietary protocols. Both RTU's and PLC's operate autonomously on the near-real time control of the process, using the last command given from the supervisory system. Failure of the communications network does not necessarily stop the plant process controls, and on the resumption of communications, the operator can continue with monitoring and control. Some critical systems will have dual redundant data highways, often cabled via diverse routes.

5.1.5 Human-machine interface (HMI)

The human-machine interface is the operator window of the supervisory system. It presents plant information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the plant being controlled, and alarm and event logging pages. The HMI is linked to the SCADA supervisory computer to provide live data to drive the mimic diagrams, alarm displays and trending graphs. In many installations, the HMI is the graphical user interface for the operator, collects all data from external devices, creates reports, performs alarming, sends notifications, etc.

5.2 SCADA generations

There are different types of SCADA systems that can be considered as SCADA architectures of four different generations that are presented in the following sections.

5.2.1 Monolithic or Early SCADA Systems

Minicomputers are used earlier for computing the SCADA systems. In earlier times, during the time of first generation, monolithic SCADA systems were developed wherein the common network services were not available. Hence, these are independent systems without having any connectivity to other systems.

5.2.2 Distributed SCADA Systems

In the second generation, the sharing of control functions is distributed across the multiple systems connected to each other using a local area network (LAN). Hence, these were termed as distributed SCADA systems. These individual stations were used to share real-time information and command processing for performing control tasks to trip the alarm levels of possible problems.

5.2.3 Networked SCADA Systems

The current SCADA systems are generally networked and communicate using wide area network (WAN) systems over data lines or phone. These systems use Ethernet or Fiber Optic Connections for transmitting data between the nodes frequently. These third generation SCADA systems use Programmable Logic Controllers (PLC) for monitoring and adjusting the routine flagging operators only in case of major decisions requirement.

The first- and second-generation SCADA systems are limited to single site networks or single building called as sealed systems. In these systems, we cannot have any risk compared to the third generation SCADA systems which are connected to the internet causing the security risks.

5.2.4 Internet of things (IOT)

In the fourth generation, the infrastructure cost of the SCADA systems is reduced by adopting the internet of things technology with commercially available cloud computing. The maintenance and integration are also very easy for the fourth generation compared to the earlier SCADA systems.

The security risks in the case of decentralized SCADA implementations such as a heterogonous mix of proprietary network protocols can be surpassed using the open network protocols such as transport layer security (TLS) inherent in the internet of things which will provide comprehendible and manageable security boundary.

5.3 Data acquisition implementation

SCADA automatically compiles and delivers information about production processes to a central hub. This system sends digitized information in real-time, and it also automatically compiles backlogs of all collected data for easy analysis later. This is known as a process historian and commonly uses a structured query language (SQL) database.

Collecting data regarding plant and machinery performance allows detecting potential problems before they affect the workflow. At their core, SCADA systems rely on programmable logic controllers (PLCs) and remote terminal units (RTUs). PLCs and RTUs communicate with objects like machines and sensors within the process and send gathered information to central processing hubs. These central processors analyse the data and distribute it to the appropriate parties.

6 Possible cyber-risk mitigation actions

6.1 Cybersecurity Framework

Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems. Cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

To manage these issues the National Institute of Standards and Technology (NIST)[4] developed and kept updated a Framework (NIST 2020) that uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs.

The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the internet of things (IoT). The Framework can assist organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

- describe their current cybersecurity posture;
- describe their target state for cybersecurity;
- identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- assess progress toward the target state;
- communicate among internal and external stakeholders about cybersecurity risk.

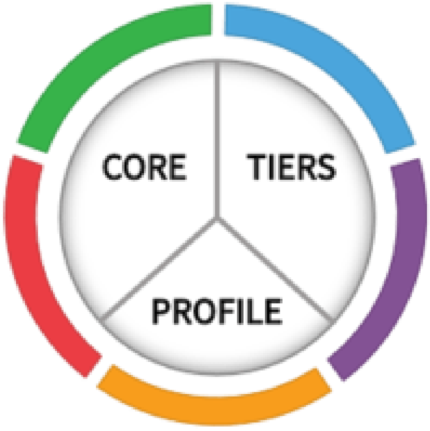

Figure 2: Components of the Framework to manage cybersecurity risk. Source: (NIST 2020)

[4] https://www.nist.gov/

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They also will vary in how they customize practices described in the Framework.

The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities.

These components are:

- the Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions:
    - Identify: develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy;
    - Protect: develop and implement appropriate safeguards to ensure the delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology;
    - Detect: develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes;
    - Respond: develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements;
    - Recover: develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning, Improvements and Communications.
    - When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for

each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

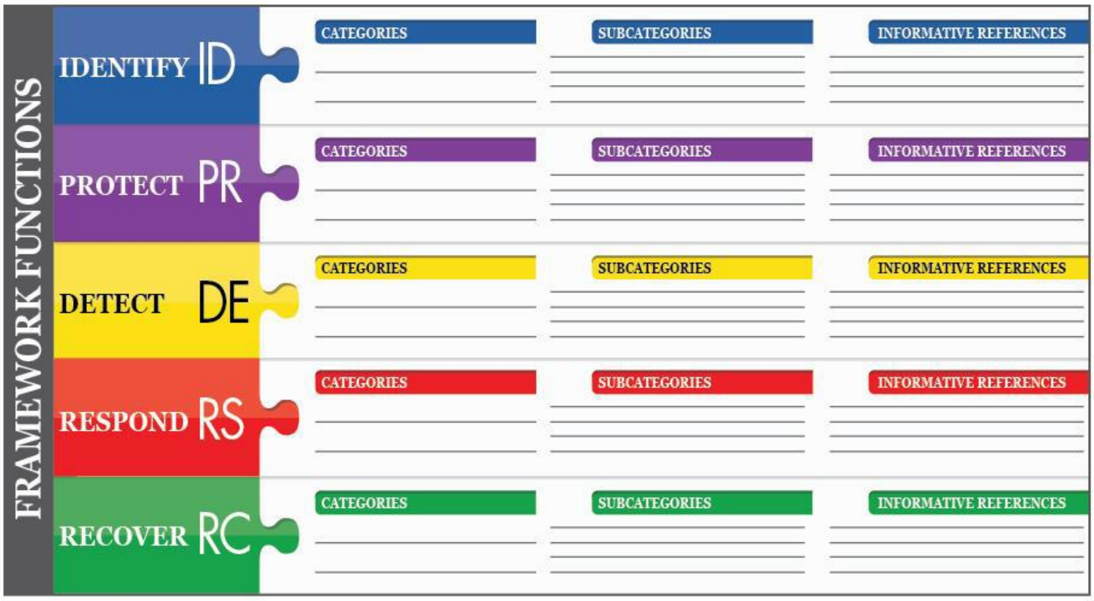

Figure 3: Functions as cybersecurity activities of the Framework Core. Source: (Calì 2019).

- Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g. risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practice over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. The Tier definitions are as follows:
    - Tier 1: Partial
        - Risk Management Process – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
        - Integrated Risk Management Program – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
        - External Participation – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The

organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

- Tier 2: Risk Informed
    - Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
    - Integrated Risk Management Program – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring.
    - External Participation – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses but does not act consistently or formally upon those risks.
- Tier 3: Repeatable
    - Risk Management Process – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
    - Integrated Risk Management Program – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possesses the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors the cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
    - External Participation - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

- Tier 4: Adaptive
    - Risk Management Process – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.
    - Integrated Risk Management Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement the executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.
    - External Participation - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs the continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

- A Framework Profile ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

6.2 Data encryption mechanism creation

Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission. Encryption is often applied in two different forms, a symmetric key or an asymmetric key. A symmetric key, or secret key, uses one key to both encode and decode the information. This is best used for one to one sharing and smaller data sets. Asymmetric, or public key cryptography, uses two linked keys – one private and one public. The encryption key is public and can be used by anyone to encrypt. The opposite key is kept private and used to decrypt.

A Policy on the use of cryptographic controls is necessary and a key management lifecycle should be adopted in order to prevent problems in data encryption.

Data encryption is necessary for communication between devices over a public network.

6.3 Other cybersecurity strategies

The cybersecurity framework, developed by NIST and the community, defines a set of steps to check, in order to assure a good response to most of the cyber attaches.

Some of the most important checks to do, interesting for the platforms under development in the REWARDHeat project are:

1. Inventory of assets.

It is important to create an inventory of each asset that composes the cyber environment that could be a victim of any type of cyber-attacks. The inventory must be accurate and kept up to date.

2. Ownership of assets.

All information assets must have a clearly defined owner who is aware of their responsibilities. The distributed assets should be managed too.

3. User registration and de-registration.

User registration should be made available and managed.

4. User access provisioning.

The user authentication process will assign access rights for all user types and services.

5. Management of privileged access rights.

Privileged access accounts should be managed and controlled.

6. Review of user access rights.

Access rights to the assets should be reviewable and updatable.

7. Removal or adjustment of access rights.

It is required a process to ensure user access rights are removed on termination of employment or contract, or adjusted upon change of role.

8. Secure log-on procedures.

Each remote or administrative activities must be access controlled by a secure log-on procedure.

9. Password management system.

Password management must be activated, and the password control check must require a complex password.

10. Controls against malware.

All the different assets in the environment must have processes to check malware in place and prevent malware spreading. Processes and the capacity to recover from a malware infection should be installed and configured.

11. Information backup.

The platform must have an agreed backup policy. This policy must comply with relevant legal frameworks.

The backups will be made in accordance with the policy and tested.

12. Event logging.

Events should be registered in an event log and the logs should be maintained and regularly reviewed.

13. Protection of log information.

Logged information should be protected against tampering and unauthorized access. Logs must be stored as long as defined in the policy.

14. Administrator and operator logs.

System administrator and operator logs should be created, maintained, protected and regularly reviewed.

15. Installation of software on operational systems.

The installation of any type of software should be controlled.

16. Network controls.

A network management process should be defined.

17. Securing application services on public networks.

Any applications which send information over public networks should appropriately protect the information against fraudulent activity, contract dispute, during the system development lifecycle.

18. System security testing.

Systems or applications developed should overcome security tests as part of the development process.

19. System acceptance testing.

A process to accept new systems/applications or upgrades should be established.

6.4 Dedicated access control creation

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

Access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors. Multifactor authentication, which requires two or more authentication factors, is often an important part of the layered defence to protect access control systems.

A very popular tool for information access control is a Virtual Private Network (VPN). A VPN is a service that allows remote users to access the Internet as though they were connected to a private network. Connecting to the VPN also protects against man-in-the-middle attacks.

6.5 Data transfer between device and cloud

The data transfer between the controller and cloud is performed by sending data periodically to the cloud server over https. There is a lot of room for improvement in this area in terms of optimization and security. Ideally, the data should be synced with the server as soon as the device is able to create a connection. This should be done securely either via a VPN or some other secure cloud data transfer protocol.

6.6 System architecture and security aspects

The defined architecture of the platform comprises two main parts, the remote device/controller and the central server.

The remote devices are connected to the network by using the local connection available at the customer.

The devices communicate in three different ways:

- accepts local connection from the same network by exposing services on port 8080 where the user can make some administration activities. Authentication is required;
- send heartbeat signals to the server by using https protocol;
- send and receive data from the server by using a secure VPN channel.

The external (by the public network) access to a device is enabled by the central server which proxy some requests to the required device by using the VPN channel. All the requests cannot be executed directly to the device and authentication is required to perform each operation.

An SSH connection, via the public network, it is possible in the devices in order to recover in case of VPN failures.

The public (certificate) and private key are self-signed by a certificate authority (CA)identified in the central server.

The whole system security is adequate but can be optimized by some improvement.

The few lacks security can be managed by defining firewall rules both on the devices and the central server. Limiting the income connections to the devices by enabling local network IP classes and/or the public central server IP may improve the security of the system.

The use of public and certified Certificate Authorities to generate the security certificate and keys can improve the security proposed to the user.

Logging and event detection may be improved and should follow standard guidelines related to the information collected and the storage lifetime.

7 Conclusions

This document guides DHC operators in the implementation of cybersecurity strategies in their systems through a risk assessment methodology and the provision of information to build a robust SCADA system for the control and operation of DHC systems.

The results of the risk evaluation at two reference DH networks have shown that the control room is the most sensitive element of DHC systems to both cyber and physical attacks. Among the cyberattacks the most threatening are: damage by third party, the failure or disruption of communication links and of main supply functions.

Among the mitigation actions that can be applied against cyberattacks, data encryption mechanism and dedicated access control are some of the suggested options.

8 Literature references

AGFW, BDEW. 2018. Industry specific security standard for the distribution of district heating, original: Branchenspezifischer Sicherheitsstandard für die Verteilung von Fernwärme (B3S VvFw). AGFW.

Calì, Federica Maria. 2019. «Un approccio olistico alla Cybersecurity nazionale.» ICT Security magazine. 8 October. https://www.ictsecuritymagazine.com/articoli/un-approccio-olistico-alla-cybersecurity-nazionale/.

EECSP, Energy Expert Cyber Security Platform. 2017. «Cyber Security in the Energy Sector. Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.»

EPRS, European Parliamentary Research Service. 2019. «Cybersecurity of critical energy infrastructure.»

IEC, International Electrotechnical Commission. 2013. IEC61131 Programmable controllers – Part 3: Programming languages. Genève: International Electrotechnical Commission (IEC).

NIST, National Institute of Standards and Technology. 2020. Cybersecurity Framework. https://www.nist.gov/cyberframework/new-framework.