A study of Secure Remote Supervision of Critical Infrastructure using Unidirectional Communication

Mateusz Chmiel,

Summary
This paper discusses the advantages of using unidirectional communication in case of remote supervision of critical infrastructure. This paper discusses proposed solution in reference to IEC 62443 standard and defense in depth strategy. It also show the advantage of discussed solution over commonly used firewalls. In the final part it was confirmed that this is not only a theoretical consideration, but also working solution that can be implemented based on available solutions - one of them has been mentioned and characterized along with a discussion of its configuration. The purpose of this paper is to prove that unidirectional communication significantly improves security of critical infrastructure and that this solution should be required if there is provided remote access to monitor elements of SCADA oriented network from external network.

Key words:
unidirectional communication, secure remote supervision, remote access, VPN, network security.

1. Introduction

Remote access to resources located in internal network is more and more often not only convenience, but even becomes necessary. It is possible to distinguish access for own employees of the company (organization) whose employer can train and impose appropriate procedures and access for persons from third-party companies (eg due to maintenance contracts, service agreements or supervision due to warranty conditions), whose appropriate behaviors are difficult be to enforce.
The risks associated with the above can be mitigated in IT networks, most often by making a proper backup, which can be recovered after failures or cyber attacks. Security compromise is almost always accepted in the IT networks. This network and access to it are secured as much as possible, but at the same time some risk is accepted.
In the operational technology (OT) networks, i.e. those whose components are Supervisory Control And Data Acquisition (SCADA) systems or, in a broader context, Industrial Control Systems (ICS), the security compromise is usually unacceptable and backups are often not sufficient.
In general, operational technology networks are related with critical infrastructure, often with a large range and are found mainly in the electric, gas, water, fuel industries and so on. The basic components of the operational technology networks are SCADA systems that form industrial and critical infrastructure. Failures or incorrect operations inside this infrastructure, eg caused by cyber attack, may result in damages that can not be repaired by recovering from backup. These could be damages that cause damage to physical elements or even threaten human health and life - these are values that can not be recovered from a backup, thus the safety and security of these resources requires uncompromising solutions.
At the same time, the convergence of OT and IT networks is a noticeable process that leads to opening the first ones for communication with external networks. This is often related with obtaining access from the external network to the OT network resources.
Previously, OT networks were closed, separated from threats from outside. Nowadays, access from outside this network is at least partially allowed, for example for monitoring in accordance with service and warranty agreements with vendor or system producer. This situation causes OT networks to be exposed to threats that previously were completely unknown to them.
It is worth noting that the primary function of the OT network is mainly connect the devices in a separated network and to realize automation [1].
Therefore, there is a need to apply appropriate security measures already in the higher layer. This paper discusses the advantages of using unidirectional communication in case of remote supervision of critical infrastructure.
In traditional IT networks security is defined by acronym CIA, what means Confidentiality, Integrity, Availability, while in OT networks security is defined by acronym AIC, because availability is the most important, second is integrity, and the last in hierarchy is confidentiality.
Therefore, it is necessary to apply appropriate security and protection measures that will prevent or significantly hinder the occurrence of any undesired events.
If a third-party company needs remote visibility of systems for monitoring or supervising the SCADA elements in which this company is responsible for, it is right to provide this access only in the minimum required range. Thus, one-way communication from the operational technology network to the IT network (or Internet through which third-party companies will be able to remotely monitor the devices and systems) will be sufficient. Any changes will force contact between employee of an

Manuscript received June 6, 2020
Manuscript revised June 20, 2020

external company and engineer on site, who will supervise if these actions are carried out in accordance with internal procedures. This type of communication could be even necessary, because any undesirable packet transmission in SCADA environment may cause a risk to availability, integrity and confidentiality in operation.
The purpose of this paper is to prove that unidirectional communication significantly improves security of critical infrastructure and that this solution should be required if there is provided remote access to monitor elements of SCADA oriented network from external network (including VPN from the Internet network).

2. The evolution from isolated operational technology (OT) networks to interconnected OT and IT network (or even connected with Internet network)

Operational technology networks at the beginning were designed as closed networks, isolated from the external environment. The main criterion was their simplicity of communication and reliability. The safety of communication protocols was less important.
However, over time, these networks have evolved and were gradually merged with office (IT) networks, for example due to the convenience of monitoring or transferring data from technology systems to office systems in which the so-called business uses this data, among others for the purpose of the analysis.
While in IT networks the lifetime of solutions is estimated for about a few years (usually from 3 to 5 years), in OT networks systems could be used for a very long time, sometimes up to 20 years and more. The necessity of their continuous work and reliability often makes it difficult to plan service breaks or even make it impossible to upgrade version of these systems. All of this contributes to creating circumstances in which these systems in the OT are not secure, unless they are adequately separated and secured in an earlier zone.
In an ideal world, these both networks remain separated, and an employee who needs to works on IT and OT systems simply has two independent workstations - the first for IT resources and the second for resources in the OT, but there is no communication between them. Furthermore, engineers from external companies come to the site and do their job locally from well-protected devices, not connecting their own devices to the internal OT network. Of course, such a situation is unattainable. However, the convergence of OT and IT networks is a progressive process. There are OT networks that are still completely isolated from the IT network. However, the general tendency rather points to the convergence between these both network, which results, for example, from the need to improve business processes. Unfortunately, this also leads to a significant increase in threats to SCADA oriented infrastructure, because it was exposed to threats and attack that were never faced before.
One of the most noteworthy examples is the situation from 2015 regarding the cyberattack on the critical infrastructure of Ukraine.
BlackEnergy - this is what the cyberattack on SCADA environment from December 2015 on the Ukrainian power grid was called, which caused power outages. The result of this attack was 230,000 people in the West of the Ukraine without power for many hours. [2]
It started quite standard from phishing, which used an e-mail with a prepared attachment containing malware. Awareness of risks is a major factor in protecting critical infrastructure. Malware does not have to be delivered directly to the infrastructure that is the target. It can be delivered first to the someone's device that has access to this critical infrastructure and will consciously or unconsciously transfer malware from an untrusted source to a network that should be secure. This risk is related with both own employees and people from external companies who, while performing remote work, connect from their computers to the network in which operate the elements of the OT network.

3. Protection of SCADA and ICS networks in a defense in depth strategy based on the IEC-62443 standard (formerly ISA-99)

The less the isolation of operational technology networks from office networks (or even Internet network), the greater the risk of potential attacks. If there is necessary to strive for the convergence of both networks, it is important to remember at the same time about the activities that will mitigate the risk related to this convergence.
There are various standards, guidelines and best practices regarding cybersecurity for SCADA. Some of them are local in nature and are often intended to a specific area of the OT network. Others are international, usually specify guidelines at a higher level - they are not very detailed, rather define general guidelines. However, it is difficult to determine a single standard entirely matching to a specific organization environment. The right strategy should be a combination of high level guidelines, own experiences and detailed requirements for a specific environment.
There is no one type, the characteristics of the operational technology network environment. It is possible to define its general features, but in detail in each company or organization this environment may be different. Nevertheless, there is a consensus on the adoption of the defense-in-depth strategy as a reference point.

The actual application of standards to a specific SCADA environment means the need to apply different standards at the same time. [1]
Solutions based on a single point of defense are doomed to failure if this single point will fail or be compromised. For example, if this point were a firewall, breaking its security (or even incorrectly configured security policies) would result in access to the entire network.
A properly designed defense in depth results in reliable security for the ICS infrastructure by collectively hardened network, control devices and systems, while addressing their performance, reliability, and safety requirements [1].
One of the most popular standards is IEC 62443 (formerly ISA 99), which specifies requirements and introduces the concepts, models and terminology for defense in depth strategy. The IEC 62443 standard focuses on SCADA and ICS, i.e. in general sense: industrial automation and control systems. [3]
Integration of IT and OT networks usually leads to reduced security. Merging this two type of network enforce the necessity of applying effective security countermeasures.
A noteworthy solution is device providing unidirectional communication, because it introduces additional separation and segmentation of the network, what is in line with the defense in depth strategy, and additionally physically allows communication in only one direction, which was expected during the implementation of the solution (usually from a separated network to a less trusted network).
Unidirectional communication makes it possible to provide secure remote supervision of critical infrastructure without exposing this infrastructure to threats from the external environment, which in fact not only mitigates the associated risks (resulting from remote access), but even eliminates such threats.

4. Security improvement by using unidirectional communication

If in the earlier described situation, regarding critical infrastructure of Ukraine, the office network and operational technology network were properly separated, then the attack vector by phishing e-mails would not work. Moreover, if a device that only allows one-way communication was used, it would be impossible to simultaneously deliver and control the malware.
Having regard to the above, it is necessary to protect the resources of the OT network already at the level of access to them.
The use of unidirectional communication allows to transfer data from a trusted network (or subnet) to a network that is less trusted - at the same time preventing communication in the opposite direction, which is undoubtedly an advantage if there is a need to share something outside, but without the possibility of accepting communication in the opposite direction.
Of course there are tasks that may require remote access. But if it is possible, and in the case of remote supervision of critical infrastructure it is possible, definitely unidirectional communication should be used, improving the level of security. Then only what should be available outside will be made available, but there is no risk that something will be sent in the opposite direction - even if there will be such an attempt, the physical construction of unidirectional communication devices will not allow it.

5. Isolation of OT and IT networks and access for service and warranty purposes

Threats are often targeted and are able to impact critical infrastructure if this infrastructure is not adequately secured or if there is a possibility of human mistake that could be avoided. Targeted attack are usually prepared for a long time, including detailed reconnaissance and finding a way to get into the internal network.
There is a risk even when using the approach with the appropriate separation of OT and IT networks.
Malware does not have to be delivered directly to the operational technology network. The first target may be a user who remotely connects to the OT network. The malware can be delivered to the user's computer, which subsequently uses a remote access connection to the resources in the OT network, thus allows malware to penetrate into this OT network bypassing the firewall rules.
Service and warranty access can be carried out remotely, at least for initial verification and monitoring. This results in cost reduction and faster response time than sending an engineer to work on site. On the other hand, it allows to go through the protected point between the OT and the external network and get to the designated segment in the OT network. That is why it is so important to properly secure communication between the OT network and external networks.
In matters of security of critical infrastructure, it should not be so easy to compromise as it is in office networks, because the consequences are radically different.
Cyber attackers use more and more sophisticated methods, while the basic critical infrastructure often is aged and uses old technology, which has been designed with less attention to the issue of security itself, consequently, in many cases, it facilitates attacks even with simplified forms of cyber attacks. The use of anti-virus software is not sufficient protection, because such solutions are usually based on attack signatures, so they protect only when someone provides them with indicators, which

causes them to cope badly with new malwares until they are recognized.
The attacker has the ability to take direct control of circuit breakers by using the industrial communication protocol, this means that power stations, gas plants, transportation control systems are all potential targets. [2]
Keeping in mind the potential consequences, the need to apply proper protection and minimize potential vulnerabilities should be noticed again.
On the other hand, in some situations, there is a need to allow monitoring of the resources of the secured network from the external network, then measures should be taken to ensure this possibility only to the minimal required scope.
Thus if it concerns a situation when it is not justified to remotely modify OT systems, there should be used a solution that allows only for remote visibility, but without the physical and technical possibility of remote interference in critical infrastructure systems without the participation of a trained engineer on site who knows the internal procedures in the company. It is easier to enforce appropriate behavior patterns and supervision over employees of own company than employees of external companies.

6. The advantage of unidirectional communication over commonly used firewalls

Commonly used firewalls provide control over network traffic, but they are not always fully secure. The operating system on which they are built may have various security vulnerabilities that can affect the operation of the firewall. Modern firewalls in addition to the standard functionality also have additional security modules, such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Anti-Virus (AV) - all of them also can have vulnerabilities. There is also the risk of human mistake. The administrator could define firewall policies that allow traffic that should not actually be allowed. There is also the risk of compromising the administrator password, and then the person who gains this password can make any changes to the firewall.
Often during sophisticated attacks, control commands are not initiated from the outside, but a computer from the internal network communicates with an external address from an untrusted network (usually via the Internet) and asks for commands to execute or additional files that it wants to download. In this situation, the traffic is initiated from the internal network, so even if the firewall blocks traffic to the network, stateful firewalls will pass traffic in the described situation, because it was initiated from the internal network (assuming that the administrator allowed internal network devices to communicate outside).
In situations where unidirectional communication is sufficient, it is recommended to use security devices also known as data diodes. This solution restricts the network communication only to the transmission in one direction. This is the result of a physical design that assumes the use of optical fiber-based standard connectivity. [4]
In simplified terms, the device is built of a transmitting module and a receiving module. Between these modules is a fiber optic link. Even if someone would like to send anything in the opposite direction, there is no physical possibility, which automatically eliminates some of the risks associated with the use of firewalls.
Remote Desktop Protocol (RDP), Secure Shell (SSH) and some kinds of shared session software are interactive remote access tools, that allow execute commands into distant environment. These capabilities also could be used for cyber attack. The use of unidirectional communication makes sophisticated remote control attacks physically impossible.[5]

7. Commercial products of unidirectional communication and remote supervision on the example of the Waterfall Security solution

The review of commercial products confirms the ability of unidirectional communication to provide remote visibility and monitoring based on screen sharing. For example, Waterfall Security Solutions Ltd. describes this as a Remote Screen View (RSV) in its portfolio.
Waterfall Security Solutions is the producer of a solution known as Waterfall Unidirectional Security Gateway. This solution consists of four components: two hosts (TX and RX) and two hardware modules (TX and RX hardware modules). The hardware modules are wired directly between the hosts with no intervening switches. These hardware modules are physically able to send in only one direction. It is important to note that only unidirectional communication between TX and RX hosts is possible, from TX to RX. Unidirectional Gateways can replicate and emulate many kinds of servers and devices, including general purpose servers and typically industrial devices, such as Modbus or DNP3 devices.
The Waterfall uses a unidirectional fiber optic link to data flow from one network, usually an industrial network, to external networks. Due to the design of the hardware, communication in the opposite direction is physically impossible. This solution eliminates any threats caused by incoming malware, thus protecting critical resources and at the same time allowing remote supervision of critical infrastructure. [6]
Remote Screen View connector is a solution that fits the issue discussed in this paper. This solution could be used to provide employees of third parties with a remote view

of those critical infrastructure resources to which they must have a remote visibility of. For example, as part of service and warranty agreements, it may be necessary to provide a remote visibility of equipment operation parameters in order to correct irregularities in their work, even before a real failure occurs.

In the above scope, a remote visibility is often sufficient, therefore unidirectional communication can be successfully used in this scope. A person outside the company or organization will see a screen preview from the system that they need to monitor, but will not be able to make changes themselves or perform other operations unauthorized by the administrator managing the subnet or a specific object in the critical network.

Third parties should not decide when and what to change. Any changes to the configuration should be made in consultation with the critical infrastructure administrator. After noticing the irregularities, joint work should be planned or staff should be instructed on how to make the proper corrections. In this way, an employee and a third party engineer cooperate and control each other as part of carrying out work in accordance with technical and procedural requirements.

8. Configuration and technical details of Waterfall Remote Screen View

This chapter discusses configuration and technical parameters defined in case of using Waterfall Unidirectional Security Gateway with a predefined connector named Remote Screen View.

This connector allows to capture the screen view from the host in one network and presents captured view on the hosts from the other network. Screens are accessed by web browsers, using video streaming applications. [6]

It is required to install software to capture the screen view on the host in the first network, but there is no need to install any client software on the hosts in the second network .

The Waterfall Screen Capture agent should be installed on the device from which the captured screen will be sent. This agent is responsible for capturing the screenshot and sending it through the Waterfall Unidirectional Security Gateway to another network or subnet.

The configuration of the agent on the source host is simplified to determine the port number for transferring screenshots, frames per minute and quality (in percentage from 0 to 100).). There are also optional options to capture the mouse and to start capturing after starting the host system. The agent from the source host displays information about sent and lost frames and frame size.

The next step on the TX host should be to define a new connector for Remote Screen View and of course to activate it. There should also be a specified channel ID (the same for TX and RX hosts), channel name and source parameters such as IP address and port number (specifying the host on which the agent is installed to capture the screen view). There are two more fields to fill: keep alive the timeout specified in millisecond and streaming URL.

After configuring the connector and applying the configuration, a new entry will appear in the Waterfall Console in the Operating Channels section, which allows to monitor bytes, packets and also alerts and network errors.

On the RX host, there should also be a new connector defined - Remote Screen View Server. During configuration, the options should be set as before, especially the same channel ID used for communication between TX and RX hosts. There is also the need to specify the channel name, port, streaming URL and keep alive the timeout specified in milliseconds.

After configuring the connector and applying the configuration, a new entry will appear in the Waterfall Console in the Operating Channels section, which allows to monitor bytes, packets and also alerts and network errors.

The above makes it possible to, for example, deploy the monitoring function from SCADA's environment to another network for monitoring control system components in real-time by third party vendors with implementation of unidirectional communication.

9. Conclusion

Through the above discussion, it was proven that unidirectional communication is at least recommended when there is communication from an operational technology network, which is part of critical infrastructure, to a less trusted network. This is at least a recommendation, because it would be reasonable to say that it should be necessary.

The situation with a cyber attack on SCADA from December 2015 on the Ukrainian power grid, as a result of which 230,000 people in the West of the Ukraine were without power for hours, shows the scale of problems related to the convergence of OT and IT networks.

In the past OT networks were closed, so they were resistant to external threats. Now a days they are more and more often open to communication with the IT network or even the Internet. They are not wide open, rather they have to transmit some data outside. However, the use of standard firewalls does not provide sufficient security in such situations.

Better security is ensured by unidirectional communication. If there is a need to make the preview available from internal systems for service or monitoring via the Internet to the external network, then this

communication will be provided only in one direction. Regardless of the skills and determination of the person from the external network, there is no physical possibility to send anything successfully to the internal network.

Remote supervision of critical infrastructure using unidirectional communication should by applied especially for third parties, whose representatives are not covered by security training, awareness programs and internal procedures applied in the organization of the SCADA infrastructure owner.

The article shows the compliance of the proposed concept with the strategy of defense in depth, which in principle is consistent with many standards regarding operational technology networks and critical infrastructure (including IEC 62443).

Using the example of a commercial solution, it has been proved that it is possible to secure remote supervision of critical infrastructure with unidirectional communication.

References

[1] X. Zhou, Z. Xu, L. Wang, K. Chen, "What should we do? A structured review of SCADA system cyber security standards", Conference on Control, Decision and Information Technologies (CoDIT), pp. 605-614, 2017

[2] T. Ball, "Top 5 critical infrastructure cyber attacks", Computer Business Review, https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/, 2017

[3] R.S.H. Piggin, „Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security", IET Conference on Control and Automation 2013: Uniting Problems and Solutions, pp. 1-6, 2013

[4] B.S. Jeon, J.C. Na, "A Study of Cyber Security Policy in Industrial Control System using Data Diodes", ICACT2016, pp. 314-317, 2016

[5] A. Ginter, "SCADA Security – What's broken and how to fix it", Abterra Technologies Inc., 2016

[6] https://waterfall-security.com/static/Waterfall-for-Remote-Screen-View.pdf, 2018