INDUSTRIAL CONTROL SYSTEMS (ICS) AMBIGUITY?

Authored by Azeem Aleem, Gareth Pritchard, and Peter Tran

The media and general public usually refer to all ICS architectures as SCADA, this is literally and technically incorrect, however, referring to ICS"Industrial Control System" (ICS) is considered a safe catch for all terms when discussing Critical Infrastructure to avoid autocratic debates with various security voice groups.

In this blog series we will discuss the vulnerabilities within the ICS systems and also mitigation techniques associated with it

Firstly a debate that always comes on the table is **Operational Technology (OT) vs Information Technology (IT).** Unlike IT networks, OT networks can be very unique with a large array of old and new devices typically with a translation device (OPC) installed in order to ensure all devices can communicate.

IT Security ultimately revolves around cost based risks. Safety historically has not been a concern in IT, although with the widespread introduction of IOT and the ever encroaching convergence of OT and IT it's likely we will see a prioritisation of cost vs safety.

OT Security ultimately revolves around safety based risks, malfunctioning OT can and does lead to physical damage of equipment and personnel. Cost based risks are secondary to safety in OT however in cases where safefy risks are null or mitigated the risk becomes cost based by default.

1. THREAT TYPES

Latest media hype has clouded the security environment creating an ambiguity, and dizzying whirlpool of reality around the ICS vulnerabilities against cyber attacks.

The following table gives a high level overview of some of the more common ICS device types along with the perceived threat the device may be vulnerable to and a baseline risk level for the impact of a threat being realized.

Any breach on the Data Historian or OPC server should be considered critical, these are the devices which would yield a lot of sensitive information relating to the network and provide an attacker with the details needed to tailor an attack against the network following completion of the recon activities.

		Short	Long	Risk #	Threat
Data Historian	OPC	DCS	Distributed Control System	S0	Unpatched vulnerabilties
		HMI	Human Machine Interface	S1	Human
		RTU	Remote Terminal / Telemetry Unit	S2	Infection & Corruption
		IED	Intelligent Electronic Device	S2	Command & Control
		PLC	Programmable Logic Controller	S3	Physical Control
		BMI	Building Management System	S3	Physical and Enviromental Control

* OPC is a Modbus server capable of translating traffic between otherwise incompatible devices The HAVEX malware utilised an OPC device to perform discovery activities on the infected ICS network. Data Historian is typically a standard database collecting logs and data from the ICS network of devices. These events are usually related to physical activities and can be extremely granular.

S0-5 is an example attack risk factor based on ease of attack for the platform alone; this is provided as a baseline to develop a risk matrix following discovery and external / internal influences. If the ICS/DCS network is *truly & fully air gapped* the risk for the network may be reduced to S5, the threat moves to a Physical intruder / Insider Threat based risk matrix which may in turn make PLCs and BMIs a higher risk.

Scenario example: Degrading the Air Conditioning control system for a server room may be catasrophic, therefore the risk for BMI could be S0 for the physical area the control system is located in. If the BMI is physically secured to outside influence however, the risk may be lowered to S4.

2. ICS MALWARE

There are several well-known ICS related malware variants that have been recently heavily analyzed and documented; these variant serve as excellent examples in understanding ICS historical perspective and threat complexion. Some of the latest malware are:

The HAVEX RAT has been attributed to the following campaigns:

- Dragonfly (Symantec)
- Energetic Bear (CrowdStrike)
- Crouching Yeti (Kaspersky)
- Epic Turla (Kaspersky)

The most noteworthy capability of the HAVEX RAT is that it contains a module for OPC Scanning which effectively enabled it with ICS Intelligence Gathering capabilities, currently believed to be the primary purpose of the malware as no additional stages of an attack were ever discovered following this apparent reconnaisance mission.

STUXNET (WORM) and Black Energy: Both are nation-state sponsored APT attacks. They have evolved through various stages towards maturity and have been utilised in advanced targeted attacks against critical infrastrucure

The malware were distributed via:

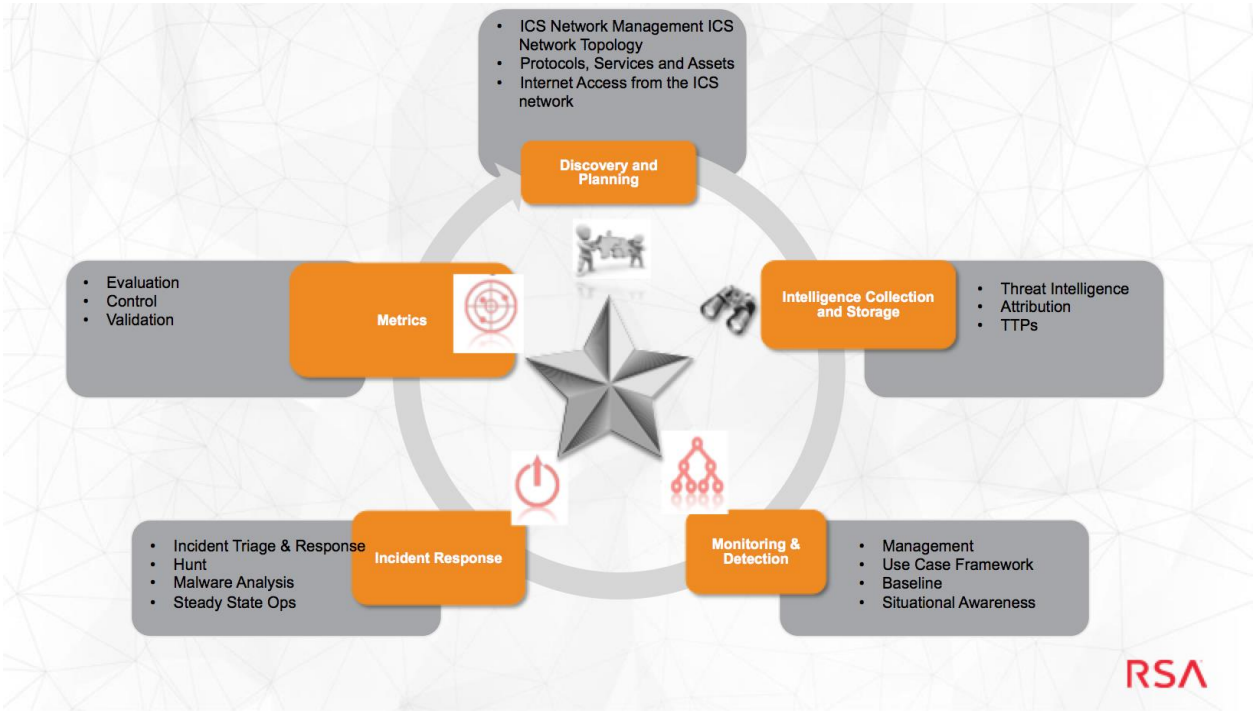
- Phishing attacks aimed at executives not on the ICS network:
  Aimed at executives not on the ICS network, the probability of successfully breaching the ICS network via this method would be low. The attacks may have been orchestrated to conduct multi tier attacks on the IT and OT infrastructure. The HAVEX RAT had ICS capability, but it was not constrained to this attack environment, it is believed to be an enhanced version of another RAT.

Wateringhole attacks on ICS vendor software delivery website:

- The exploits used on the wateringhole attacks are from Metasploit, the software was trojanised and loaded with the HAVEX RAT the attack would be reliant on an ICS engineer downloading new software from a vendor site and transferring the software directly to the ICS network without checking MD5 hashes, or verifying the package was legitimate.

3. ASSESSING THE THREAT

So where do organizations starts from to assess the threat? We need to follow a methodological framework. **Within RSA Advanced Cyber Defence Practice** we follow the domains/ framework to assess and mitigate the ICS threat.



ICS DISCOVERY AND ASESSMENT.

Base questionarieres could be useful in assessing the current landscape.The resident ICS engineer should be able to answer a set of base level questions; this would be sufficient to get started in planning required actions in setting up the ICS ASOC. The answers to these questions are sensitive, and should be marked appropriately and received via encrypted communication or kept on the customer network. If received outside of the customer network, redact or destroy the data after use.

Initial Questionnaires

Colour Key!
Green: Core question
Blue: Dependency Question (May be skipped if invalid due to previous answers)

Q/A	ICS Network Management	Notes
Q1	Is the ICS network attached or separated from the IT network?	
Q2	Are there plans within the timeline of the engagement to separate / join the ICS and IT network?	Any plans to modify the network that may affect the ongoing work to monitor the network.
Q4	If the ICS network is separated from the IT network, is it fully air gapped?	
Q5	If the ICS network is air gapped from the IT network, is it managed via ICS Wi-Fi or otherwise, how is it managed?	
Q6	If the ICS network is managed remotely, can the remote link be utilized to collect data into the CDC via a one way feed?	
Q7	If the ICS network is air gapped with no remote feed, what is the possibility of manual transference of data into a CDC accessible collector on a time schedule coinciding with typical ICS engineering maintenance duties?	
Q8	If detection is via manual reporting from an OT Engineer only, how feasible would ad-hoc manual collection of logs and / or deployment of a packet capture device on to the network be?	
Q3	Can a high-level network map be produced and / or provided for review?	Kept on the network, Encrypted communication outside of the network or eyes-only?

Q/A	ICS Network Topology	Notes
Q9	Is the network partitioned or flat?	
Q10	If flat can chokepoints switches be installed in the network in order to capture network traffic?	Open for discussion based on best placement according to visibility and equipment availability / chokepoint numbers
Q11	If flat and chokepoint switches can be installed, can a flat network map be provided in order to identify the best placement for the chokepoints?	Open for discussion based on best placement according to visibility and equipment availability / chokepoint numbers
Q12	If partitioned, can a high level network map be provided in order to identify placement of network capture devices?	Open for discussion based on best placement according to visibility and equipment availability / chokepoint numbers

Q/A	Protocols, Services and Assets	Notes
Q13	Can a list of typical / expected protocols and services be provided?	Server Services, such as OPC, Port Services such as Modbus. Include any services or ports, which should never be seen such as SSH.
Q14	If a list of protocols and services cannot be provided, can an NSM solution such as a virtual passive packet capture device be installed to collect this data?	Temporary virtual machine to collect passive information, such as Security Onion or Wireshark.
Q15	Can an asset list be provided, along with a meta tag specifying the asset type (i.e. Data Historian, OPC Server, PLC)	Kept on the network, Encrypted communication outside of the network or eyes only?
Q16	Can a list of device vendors be provided, along with version numbers?	

Q/A	Personnel	Notes
Q17	Who will be the primary contact for additional and future technical questions relating to the ICS network?	Name, E-Mail, Telephone, Hours of availability
Q18	Who will be the primary contact if a suspicious event is monitored?	

INITIAL MITIGATION

Following completion of the Q/A Baseline, the data will need to be analyzed to identify the current monitoring capability and any gaps which will effectively create blind spots on the network due to a lack of monitoring capability.

REMOTE POP ON THE ICS NETWORK.

If the discovery highlights that the network has permanent remote connectivity, this POP (Point of Presence) should be very tightly configured and monitored, and all management and change control should be vetted and verified by multiple personnel in order to ensure the network is not breached from this POP.

INTERNET ACCESS FROM THE ICS NETWORK

If ICS engineers have access to the Internet to download new firmware, there is a risk of infection directly on the network. This is a practice attackers have taken advantage of in the past. Ensuring ICS engineering HMI are segregated and never presented on the WAN or Internet would prevent incursion via this method.

Data Transference between the IT and ICS network
Any device which is used to transfer data between the Internet/IT network and the ICS network should be encrypted and presented to an air gapped 'sheep dip' machine prior to being used on the ICS network. This Sheep Dip machine should be capable of detecting any malicious or suspicious files on the media.

FLAT NETWORK

If earlier questionnaires assessment highlights a flat typology then we need to address caution. The flat network is difficult to monitor, as there are no choke points to install Network Security Monitoring devices on. The first recommendation under this circumstance would be to re-design the architecture of the network effectively zoning the network and creating monitored choke points that can be used to detect suspicious traffic occurring between the zones.

If a network map cannot be provided, creating a generic network map utilizing the collected information to show a high level before and after topology and design will help to explain and present the architectural changes required to monitor the network effectively.

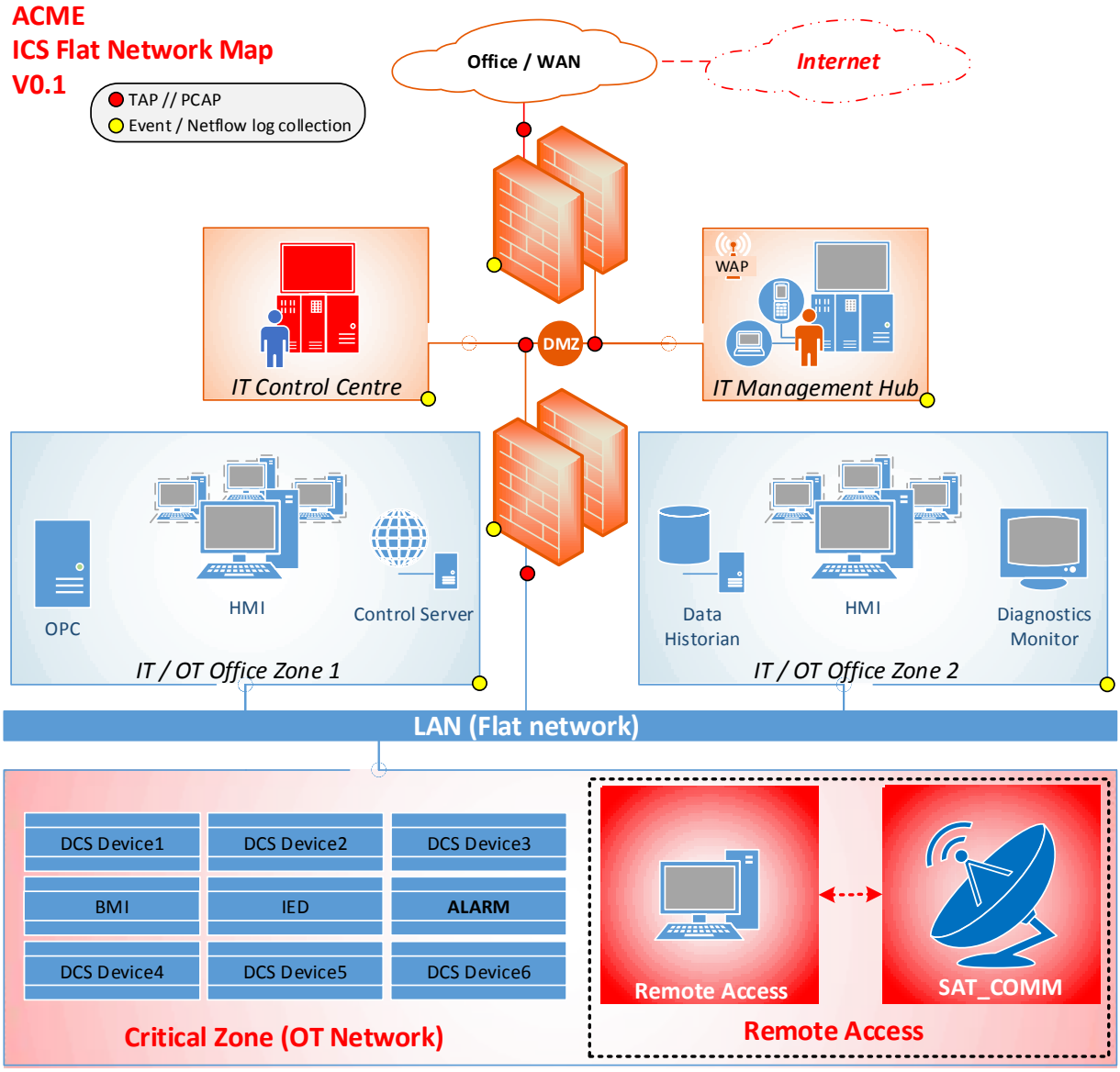


Fig1

In the above scenario, the lack of any segregated devices would remove the possibility of placing and configuring a mirrored port on a switch in order to monitor traffic. As ICS devices are usually bespoke or logical devices, they do not always generate logs; some newer devices may generate event logs, however ICS networks won't likely be upgraded often and are more likely to contain devices, which don't generate system logs. Some devices may generate physical event logs which the Data Historian collects via the OPC server, this type of event collection can be useful to correlate with system logs and network traffic, however it won't likely indicate a breach without that correlation.

In addition to the lack of adequate monitoring capabilities, an attacker gaining access to this network type would have access and visibility to the entire network with simple reconnaissance activities, and no devices to prevent devices communicating which usually would not need to communicate.

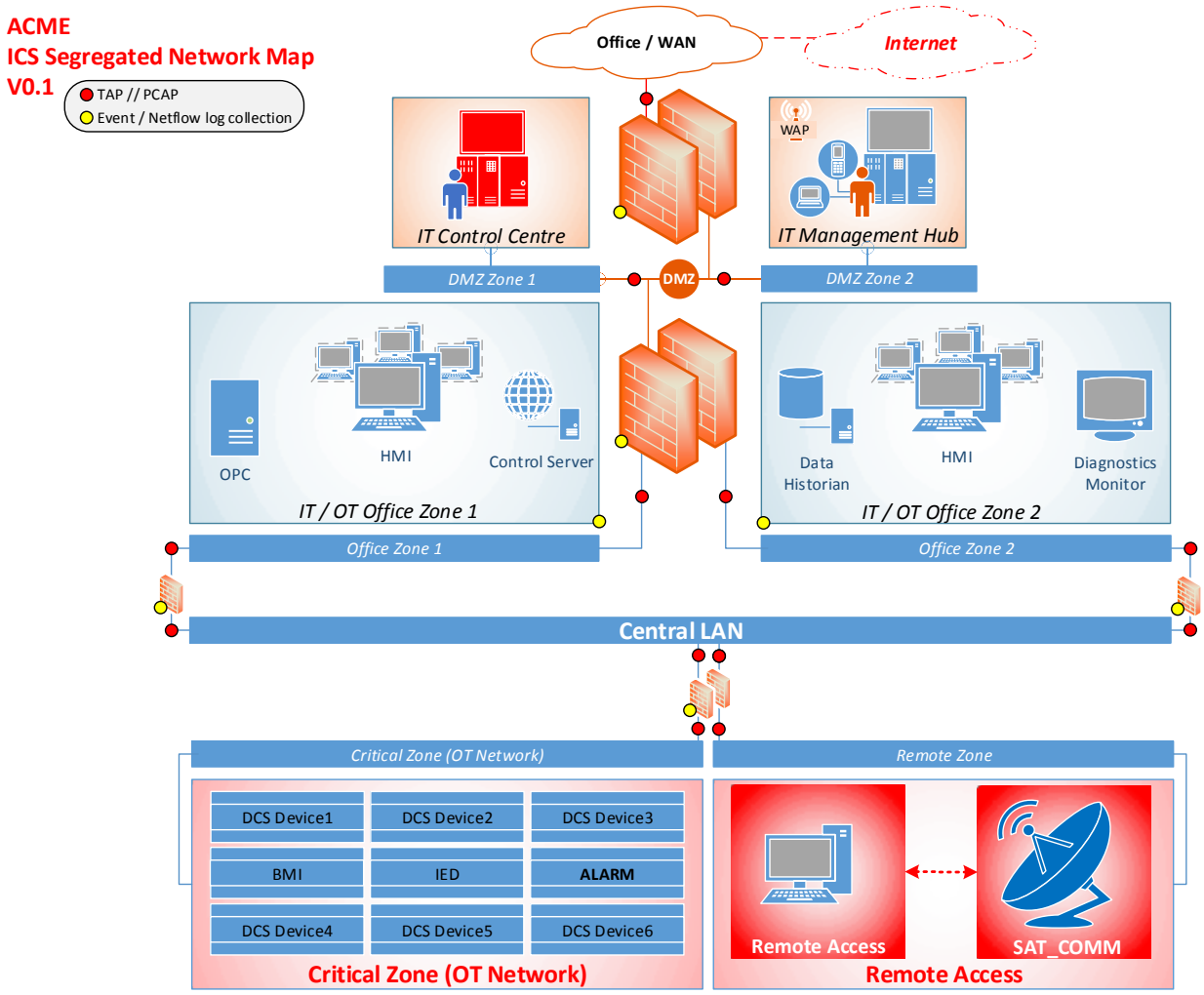


Fig2

The above example in comparison to Fig1 would be simple to install a monitoring device on. Placing switches in line between the firewall and the network segments would allow a port mirror to be configured on the switch for a packet-monitoring device to be installed.

Ideally the monitoring devices would be permanently installed. In some circumstances it could be configured as a removable device and only installed during an incident in order to provide a higher granularity of data on the segment. Performing this type of monitoring would be more useful on a very large network where outer segments are monitored on a permanent basis and inner segments are monitored ad-hoc when an incident is raised and confirmed.

Segregating the network in this manner also makes the infrastructure difficult for an attacker to map during reconnaissance; it may even prevent a targeted attack from succeeding if an infected device is unable to connect to the inner target device.

This type of disruption to an attack could provide additional time for the monitoring team to react to the suspicious events.

Unless accurate network maps have been supplied and authorized for offsite use, these maps do not need to be fully accurate. At this stage they are only intended to provide a high level recommendation and overview of the benefits in segregating the network along with monitored network capture and switching devices.

In the next series of blog we will address the other core domains.