COVER STORY

New Approach to Understanding SCADA Cyber-Security

by Ir. S. Vignaeswaran

DEFINITION OF CYBER-SECURITY

Computer security, cyber-security, or IT security, is the protection of computer systems from theft of or damage to hardware, software or electronic data, as well as from disruption or misdirection of the services they provide, with respect to all stakeholders.

If attempts are made to comply with the above across the board in any company, the cost will not only be prohibitive but the measures will also be complex, tedious and self-defeating. As such, prudence and innovation combined require that cyber-threats be defined and identified so that specific counter measures can be applied at acceptable compromises.

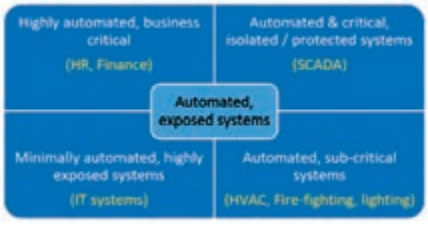
Cyber-threat is defined as "the possibility of a malicious attempt to damage, disrupt a computer network or system, deny access or steal information".

This definition, though more concise, places the impact of all cyber-threats, irrespective of their origin, on an equal footing. It is not the correct approach for SCADA systems and therefore, it has to be refined with the weightage of the potential source of cyber-threats and the SCADA impact. It has to be explicitly stated that SCADA is **NOT** an IT system but is related to it. Unfortunately, all if not most cyber security measures are for IT and not SCADA systems specifically. This metaphorical kitchen knife being in the bedroom is an issue and concern that is being addressed here.The best way to protect systems is to do a cyber-security scoping.

CYBER-SECURITY SCOPING

The scope of the cyber-security has to be established and defined precisely for maximal effectiveness. This allows for the focusing of solutions towards only the area of vulnerabilities, thereby reducing cost and increasing simplicity.

However, this depends on the level of computer automation and the level of cyber-threat that can be imposed upon it. As such, cyber-security approaches will differ from system to system, just as the perspectives to risk differ from company to company.



Even within real-time online systems, we have fire-fighting, HVAC, telecommunication, lighting etc. systems that may or may not fall under the cyber-security system coverage. So, segmentation of the potential cyber-threat targets is an essential part of the evaluation process.

WHY SCADA CYBER-SECURITY IS IMPORTANT

The objective of SCADA cyber security is to funnel all system threats away from the critical, operational and end-user systems for the purpose of elimination. Utility, production line and business SCADA systems are continuously operating systems that continuously generate revenue for the business entity. As such, its unanticipated downtime is not only unacceptable but it can also be unaffordable, like that of a nuclear reactor. To put it in another way, SCADA systems are computer systems that oversee the generation of corporate revenue by controlling the relevant processes or productions.

The risk to a SCADA system is the impact of not fulfilling its deliverables correctly, consistently and in a fail-safe manner.

CYBER-THREAT CIRCUMSTANCES

There were several technology trends driving the cyber-threat landscape in 2018 and into 2019.The basis for these trends is as follows;

i. The computer is superior to humans in so many ways that it is impossible to get anything done without them. It is this extreme reliance on them that has caused cyber-threats to be ever present in our lives.

ii. The computer works so fast, accurately and without rest that it

does not allow human intervention or supervision as desired. The computer applications are result-orientated more than correct process orientated. The correctness of process is basically programmed in and it is this that carries with it the human errors and weakness, to be exploited by the cyber-threats. All this is done with the speed of computing which makes cyber-threats undetectable to the humans until it is too late or it manifests itself in a humanly detectable manner.

iii. Computer networks, systems, Internet, application programming etc. are man-made and so have inherently human flaws built into them. Therefore, the cyber-threats exploits these inherited DNA flaws. Using more humans to offset the "computer flaw" only increases instead of decreases cyber-security threats.

iv. We are increasingly dependent on standardisation of networks, protocols, data, application etc. It is this standardisation that allows cyber-threats to use the consistencies, to affect many people, many places, many times over. Does this mean that we should abandon the notion of standardisation?

v. Computer interconnectivity has reached a level where being "not connected" is considered "out-of-place" and unacceptable at times. This has allowed cyber-threats to reach the masses in a multitude of ways, simultaneously and instantaneously.

vi. Lifestyle digitalisation has seen TV, phones, radio, newspaper etc. digitalised and computerised. So now, the doors to cyber-threats includes hand phones, iPads, laptops and USB drives, among others.

To understand any problem, we as engineers, must go back to the first principles and see the root cause, the circumstances and frequency of occurrence … to be able to identify a permanently viable solution

vii. High mobility of company staff has given rise to in-house information slowly drifting to the outside world at an increasing rate. This only arms the cyber-threat even more.

viii. Centralised, cost optimised, cloud-based data storage has seen more and more confidential company information leave the physical boundaries of the company premises. This has encouraged cyber-threats in ways that were not possible before.

ix. High-speed communication mediums have allowed data and applications to travel faster than before, increasing with time "exponentially". This in turn has allowed cyber-treats to propagate at a similar rate, faster than before as well.

x. The contextual nature of computer and IT applications with respect to human values is the basis for cyber-threats. Deleting unwanted files is acceptable but deleting wanted files is not. Hence, the definition of wanted is vague, contextual, varies from person to person and it is time-based. Therefore, it is the "intent" of the computer activities that decides whether it is detrimental or beneficial. Unfortunately, the former or the latter cannot be established without letting it happen first and then only, in hindsight, judge the consequences of the actions.

xi. Solution providers often tell their clients that their applications are 100% compatible and will operate seamlessly with the current IT infrastructure, and for the most part, this is true. The problem arises when we start adding IT security solutions from different manufacturers regardless of the granularity of their configuration settings – thereby causing "technology gaps" to be always present.

No cyber-threat could ever affect or impact a typewriter … so why do we even think of protecting it? A digital calculator is not web-based to protect, a digital watch is too cheap to protect, a digital microwave has no business basis to protect and the only protection for PC is a re-format. Therefore, what we are exactly protecting is… computer availability, business functionalities and its data/information/knowledge... which are the organs and blood of a company.

xii. Technology gaps will always appear for another simple reason: Developers will always keep certain portions of their code proprietary as part of their competitive advantage. Hence, true compatibility and interoperability may only be 90% at best. It is these that are known as technology gaps and it is through these gaps that attacks usually occur.

xiii. One of the most problematic elements of cyber-security is the constantly evolving nature of security risks. The traditional approach has been to focus resources on crucial system components and protect these against the biggest known threats, which meant leaving "lower priority" components and system undefended. It is via these unprotected systems less dangerous that cyber-threats exploit.

xiv. Internet of Things (IoT) where individual devices connecting to the Internet or other networks is the buzzword and trend of things. However, it is also the very same connection to cyber-threats as well.

xv. Big data is another buzzword of the times, allowing high-speed, automated processing of enormous information stored in hand phones, laptops, Web

browser, desktops and elsewhere. These are the very means and targets of cyber-threats.

xvi. Automation of computer activities with artificial intelligence (AI) so that there is minimal human supervision required, is spreading across the IT landscape. Who has stopped to think that it is this very same AI that powers and nourishes the cyber-threats?

xvii. Modern co-operative and coordinated processing trends in IT are the very means that cyber-threats are being used to target the individuals and the collective. Gone are the days of individualistic glory hunting virus writers who boost their ego by being a nuisance.

xviii. Data is the new "oil" of the digital economy, so it is perceived by many, and like "oil reserves" that most companies are equated to, that cyber-threats mine and undermine, threatening that very commodity.

In the above, we have identified at least most of the "whys" that give rise to the existence of cyber-threats.

Now, let us look at the categorisation of the cyber-threats so that we can exploit their weakness and weaken their strengths.

CYBER-THREAT MOTIVATIONS

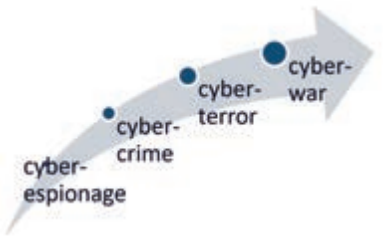
Let us look at the macro or broad categories of cyber-threats. Cyber-threats are siloed into the following groupings:

i. **Cyber-espionage** is the practice of using computer systems and information technology networks to obtain secret information without the permission from its owners or holders. Cyber-espionage is most often used to gain strategic, economic, political or military advantage, and is conducted using cracking techniques and malware.

ii. **Cyber-crime** which includes single actors or groups targeting computer systems and corporate IT networks for financial gain, directly and/or indirectly.

iii. **Cyber-terror** which is intended to undermine electronic systems and cause panic or fear. The disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes on the form of attacks on networks, computer systems and telecommunication infrastructures.

iv. **Cyber-warfare** involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. Cyber-warfare has been acknowledged as the fifth domain of warfare (following land, sea, air and space) to impair such infrastructural services as transportation and medical services or to interrupt commerce.



SCADA professionals only talk about cyber-security or cyber-threats in terms of the 4 categories listed above.

There is a cyber-threat perspective that a SCADA system is not a financial or library of confidential information system. Since SCADA systems do not have direct (banking) financial information or digital currencies, the concern about cyber-crime can be misleading. If the aspect of ransomware is included, then the notion of "being robbed without having money stolen" takes on a whole new meaning.

Cyber-espionage has the least bearing on a "pure" SCADA system. Knowing about the field devices detail only embarrasses the company in terms of its confidentiality and security aspect, which could be rectified accordingly. However, both cyber-espionage and cyber-crimes tools which are meant for generic purpose IT networks can hang, corrupt or disrupt SCADA systems unintentionally. On that basis, they are considered as threats.

National-level SCADA systems are more concerned with cyber-terror and cyber-warfare. This is because a national-level infrastructure SCADA system can be modified as a "DDOS" tool for an enhanced multi-level multi-prong cyber-attack weapon. Such Distributed Denial Of Service (DDOS) to the public has dire consequences.

Cyber-war by nations or cyber-terrorism by "pseudo-nations" has the same outcome to the intended victim with a nationalistic SCADA system. They both interrupt and threaten national security.

CYBER-THREAT MEANS

SCADA systems are self-contained business systems that need not communicate with "outsiders". Hence, they can be Web-isolated.

The purpose of a SCADA system is to automate and with that comes ever reducing human intervention. As such, human interfacing can be restricted to the maximum. The SCADA system software is specifically built for a specific purpose. So the software is "cast in stone" by functionality. There should be no need to amend, modify or enhance the software that should function like a "pencil" (in functionality) to its end-user.

Unfortunately, building SCADA systems upon the Windows platforms defeats this purpose with the default Web-access requirement for Windows update.

Nevertheless, the measures against cyber-threats include:

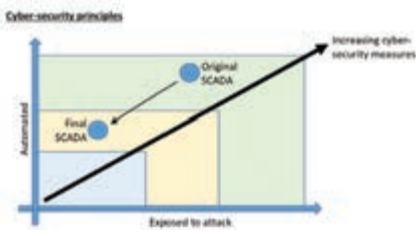
i. Eliminating web access and surfing

ii. Eliminating or minimising human access and errors

iii. Restricted patching and modifications

iv. "Technology gap" reductions

In many ways, this will be seen as a "regression" of the SCADA system.



Without going to into too much detail, the matching of the threats in the wild to the following measures has to be done with the hope minimising their potential impact.

No.	Cyber-threats	Solutions
1	Backdoor	Restricted patching
2	Denial-of-service attacks	No access & No web
3	Direct-access attacks	No access & No web
4	Eavesdropping	No access & No web
5	Multivector, polymorphic attacks	Honey-potting, No access and No web
6	Phishing	No access & No web
7	Privilege escalation	No access & No web
8	Social engineering	No access & No web
9	Spoofing	No access & No web
10	Tampering	No access & No web
11	Advanced Persistent Threats	Honey-potting, No access and No web
12	Trojans	No access & No web
13	Botnets	No access & No web
14	Ransomware	No access & No web
15	Wiper Attacks	No access & No web
16	Intellectual Property Theft	No access & No web
17	Theft of Money	Not applicable
18	Data Manipulation	Honey-potting
19	Data Destruction	Honey-potting
20	Spyware/Malware	No access & No web
21	Man in the Middle (MITM)	No access & No web
22	Drive-By Downloads	No access & No web
23	Malvertising	No access & No web
24	Rogue Software	Restricted patching
25	Unpatched Software	Restricted patching

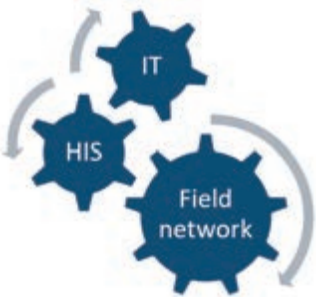
The above has to be augmented with the following layering approach to SCADA security systems, to eliminate technology gaps.

CYBER-SECURITY GAPS

i) Macro operational gaps

Threats originate from the boundaries of the SCADA system. It is unfortunate that the modern SCADA system has at least 3 interface points:

- Corporate IT system
- Field data network system.
- SCADA – human interface (HIS)

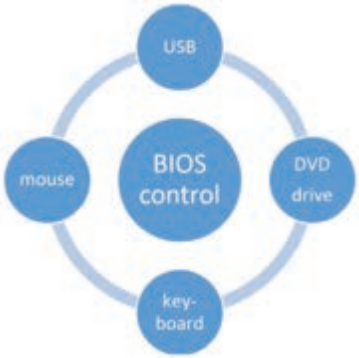


Each of these boundary points has a unique functional aspect that carries with it differing points of vulnerabilities. This is indirectly covered by the other cyber-security article in this magazine edition.

ii) Micro technological gaps

DVD drives can be locked or removed to prevent control operators from inserting CD-ROM or DVD-ROMs. The most damaging aspect is the ultra-intelligence of Windows OS to auto-run any ROM disk that is inserted into the drive. This does not allow the DVDs to be scanned first unless an anti-virus software specifically setup to do so. Even then, the 3rd party AV software is at the mercy of the Windows OS.

USB ports are a bit trickier now since both the new generation mouse and keyboards are USB based. Previously, they were PS2 socket based and all USBs on the PC can be generically blocked. Currently, the mouse and keyboard USB sockets can be interchangeable and can also be used as thumbdrive inputs.



Charging of handphones via the USB ports is highly prohibited as the wireless handsets is a serious breach of the SCADA system security requirements. This is one of the reasons why the USB ports should be physically sealed to avoid this.

The use of wireless mouse and keyboard is prohibited as their use opens up the USB port and wireless signaling for abuse.

SUMMARY

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it is necessary in order to protect information and other assets from cyber-threats, which take many forms evolving over time continuously.

The primary objective of SCADA cyber-security is to avoid being hit, not to recover from a hit. This is very different from the perspective taken from the IT viewpoint.

Cyber-threats require us to change what we have been doing in the past with past values and adopt new ways and new values. If we keep doing what we have been doing, then we are going to keep getting what we have been getting so far. ■