

Impact Driven Risk Scoring in Industrial Control Systems

04.07.2019

Author(s): Can Demirel

Version : Version 1.0, 04.07.2019



Introduction





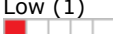
There are lots of best practices to calculate cyber security risk score. Most of the calculations are based on likelihood and impact but it is proven that general risk scoring methodologies are not good enough to address industrial cyber resilience needs. Our cyber-physical resilience experiences in the field led us to develop a lean cyber risk scoring methodology in ICS domain. It is basically impact driven and it aims to help asset owners to focus on real risks which could affect the processes.

Impact Driven Risk Scoring in ICS Domain

$$ICSR^* = Digital\ Dependency(x) \times Impact(x) \times Control\ Effectiveness(x) \times Mike\ Factor(x) \times Point\ of\ Entry(x) \times Cyber\ Security\ Severity$$

*Industrial Cyber Resilience Score

The maximum value of industrial cyber resilience score could be 15625 according to equation. Please find severity levels and their explanations on the following table.

Severity/Score	Explanation
Emergency (5) 	12501-15625 No need specific knowledge. Entry point is control network, business network or internet. Easy to damage process, people and environment. Subject to penalties.
Critical (4) 	9376-12500 Low-level process and security knowledge. Entry point is control network, business network or internet. Easy to damage process.
High (3) 	6251-9375 Requires mid-level process and security knowledge More than 2 or more complex steps should be carried out. Entry point is control network, business network or internet. Possible to damage process.
Medium (2) 	3126-6250 Requires mid-level process and security knowledge. More than 2 or more complex steps should be carried out. Entry point is control network or business network. Hard to damage process.
Low (1) 	1-3125 Requires complex process and security knowledge. More than 2 or more complex steps should be carried out. Entry point is control network or isolated network. Hard to damage process.

Dependency

Dependency parameter stands for understanding value of asset and its cyber dependencies. Dependency parameter has three different parameters and it is calculated as the maximum value of all three parameters. Please find scoring criteria for each parameter below;

Parameter\Severity	N/A	Low (1)	Medium (3)	High (5)
Industrial Dependency		There is no control system implemented. Processes are done by manual operations.	Control/Automation is implemented but it is limited.	Whole infrastructure relies on control/automation system. Control system has sub-control system and lack of control system has domino effect on operations.
Digital Dependency		Process doesn't need any computer-based infrastructure.	Computer-based systems are implemented but it is limited.	Whole processes are managed by computer-based systems.
Cyber Security Dependency		Cyber-attacks have very limited effect on the process.	Processes could be damaged by a cyber-attack but it is limited.	Processes could be damaged by a cyber-attack and also it is possible to have loss of view or loss of control effect.

$$\text{Dependency} = \max(\text{Industrial Dependency, Digital Dependency, Cyber Security Dependency})$$

Control Effectiveness

Control effectiveness stands for understanding the degree of protection mechanism and it is also used for likelihood prediction, therefore in our calculation there is no likelihood factor since it is hard to model likelihood in ICS Domain because of limited knowledge of incidents and their density. Once control effectiveness is well implemented then its degree of impact to equation should be low and vice versa.

Severity	Explanations
High (5)	Nothing is implemented or effectiveness of controls is very limited.
Medium (3)	Some of best practices are implemented. It is still possible to implement new controls or possible to improve the effectiveness of implemented controls.
Low (1)	Infrastructure is implemented according to best practices. Safety systems are implemented. Safety logics are implemented. Mechanical safeguards are implemented. IT-OT cyber-physical controls are implemented. All controls are effective and there is nothing more to be done.

Impact

It is always hard to score impact value during risk assessments. In our methodology we have added different type of impact categories to have a better calculation to understand real risks in related infrastructures. Impact factor has three main parameters and each parameter has their own sub-parameters.

Impact is calculated as the maximum value of all three parameters. Please find scoring criteria for each parameter below;

$$\text{Impact} = \max(\text{Social Impact, Industrial Impact, Corporate Impact})$$

Social Impact

Critical infrastructures often have control over physical world, therefore major concerns are not to harm people and cause any damage to the environment. If there will be any violations in these two parameters, there will be a social impact to company.

Social impact is calculated as the maximum value of these two parameters. Please find scoring criteria for each parameter below;

Parameter\Severity	N/A Low (1)	Medium (3)	High (5)
Harm to People	%xx of Company employees are affected by the incident	Almost all employees are affected by the incident and also people around the facility is affected.	A large number of people are affected by the incident.
Environmental Damage	Environmental damage is only limited to company facility	Environmental damage is not only limited to company facility but also the surrounding area.	A very wide geographical area is affected by the incident.

$$\text{Social Impact} = \max(\text{Harm to People, Environmental Damage})$$

Industrial Impact

The lack of cyber security controls has two main effect to industrial processes according to Dragos State of Vulnerability report. (Year in Review 2018 Industrial Controls System Vulnerabilities)

- Loss of view: The inability to monitor and/or read the system state.
- Loss of control: The inability to modify the system state.

Industrial impact is calculated as the maximum value of these two parameters. Please find scoring criteria for each parameter below;

Parameter\Severity	N/A Low (1)	Medium (3)	High (5)
Loss of Control	There is no direct effect on processes.	Industrial processes are affected but it is possible to recover in acceptable time frame.	Industrial processes are affected and also it is hard to recover into normal operations or it will take a long time.
Loss of View	There is no direct effect on processes.	Industrial processes are affected but it is possible to recover in acceptable time frame.	Industrial processes are affected and also it is hard to recover into normal operations or it will take a long time.

Industrial Impact = max(Lose of Control, Lose of View)
--

Corporate Impact

Corporate Impact has three different parameters and it is calculated as the maximum value of all three parameters. Please find scoring criteria for each parameter below;

Parameter\Severity	N/A Low (1)	Medium (3)	High (5)
Financial Loss	The identified finding's impact is around %xx of total revenue	The identified finding's impact is around %yy of total revenue	The identified finding's impact is around %zz of total revenue
Operational Damage	Operations can return to normal in a business day or in a matter of hours	Operations can return to normal in days or about a week.	Operations can return to normal in weeks or a month, or even more.
Loss of Reputation	It is possible to recover in short term.	It is possible to recover mid-long term.	It is possible to recover in long term or even longer.

Corporate Impact = max(Financial Loss, Operational Damage, Loss of Reputation)
--

Mike Factor*

It is a common problem to address how to start mitigations. It is often asked to us which step should be first and how to prioritize dozens of actions. In our approach we have prioritization criteria in our calculation. The parameters are taken from ICS-CERT report named "Seven Steps to Defend Industrial Control Systems_S508C.pdf" and they are divided into 3 levels as high, medium and low. This report is based on real world incident handling and response scenarios. Each parameter has a percentage value which addresses potentially mitigation rate by itself.

Since it is prioritization criteria, the minimum value of this parameter is selected as "3/Low" to have better calculations and prioritization.

*Mike Factor, In the memory of Mike Assante.

Parameter	Severity
Application Whitelisting (AWL)	High (5)
Configuration/Patch Management	High (5)
Attack Surface Area	High (5)
Defendable Environment	Medium (4)
Authentication & Access	Medium (4)
Monitor and Respond	Medium (4)
Secure Remote Access	Low (3)

Point of Entry

Point of Entry parameter is used to address how industrial threat is triggered. There are 3 different entry points in our calculation which means threat can trigger the risk from three different entry points.

- Control network,
- IT or Business network,
- Internet, WAN

Please be aware of each entry point should be related to industrial effect. For example if an internet based service is able to manipulate industrial process, it will be scored as high level on the other hand if finding requires to be connected to the control network or at to be industrial facility physical location, it will be scored as low.

Parameter\Severity	N/A	Low (1)	Medium (3)	High (5)
Point of Entry		Control network	IT, Business Network	Internet

Cyber Security Score

Cyber Security Score is one of the key factors to calculate industrial cyber resilience risk score therefore it is highly important to have a well-established methodology and scoring approach. CVSSv3 vulnerability scoring is widely accepted by the industry. In our risk scoring approach CVSSv3 is segmented into five different severity levels. Each identified finding will be reviewed according to CVSSv3 scoring and then will be put in equation as whatever the severity level it is. Please find details below;

CVSS v3 Severity	CVSS v3 Severity	Risk Scoring Severity
None	0.0	1
Low	0.1-3.9	2
Medium	4.0-6.9	3
High	7.0-8.9	4
Critical	9.0-10.0	5

Audit Domains

It is highly recommended to review following technical and non-technical domains during risk scoring. This list is taken from ICS-CERT Defense in Depth Strategies*** document.

- Risk Management Program
- Cyber Security Architecture
- Physical Security
- ICS Network Infrastructure
- ICS Network Perimeter Security
- Host Security
- Security Monitoring
- Vendor Management
- The Human Element

References

** Seven Steps to Defend Industrial Control Systems_S508C.pdf

*** NCCIC_ICS-CERT-Defense in Depth_2016_s508c.pdf