Industrial Automation Control Systems (IACS) System Testing and Assessment Rating (STAR) Methodology

Version 1.0
September 16, 2023

TABLE OF CONTENTS

1.0 Introduction 3

2.0 Risk Analysis Overview 4

3.0 Approach 6

3.1 Step 1: Identify Threats (ISA/IEC-62443-3-2 ZCR 5.1) 7

3.1.1 Threat Actor Factors 7

3.2 Step 2: Identify Vulnerabilities (ISA/IEC-62443-3-2 ZCR 5.2) 9

3.2.1 Vulnerability Factors 10

3.3 Step 3: Estimating Consequences and Impact (ISA/IEC-62443-3-2 ZCR 5.3) 11

3.3.1 Technical Impact Factors 11

3.3.2 Safety Impact Factors 12

3.4 Step 4: Estimating Likelihood (ISA/IEC-62443-3-2 ZCR 5.4) and Consequences 14

3.5 Step 5: Calculate Unmitigated Cybersecurity Risk (ISA/IEC-62443-3-2 ZCR 5.5) 15

3.6 Step 6: Reporting Vulnerabilities and Vector Scores 15

4.0 IACS STAR Calculator 17

4.1 Online IACS-STAR Calculator 17

4.2 On Premises IACS-STAR Calculator 17

1.0 INTRODUCTION

Security assessments and penetration testing of an Industrial and Automation Control Systems (IACS) / Operational Technology (OT) environment are two types of vulnerability assessments that feed information into the ISA/IEC 62443[1] risk assessment process. The Cyber Security Management System (CSMS) process, detailed in the ISA/IEC-62443-2-1 standard, requires a detailed risk assessment which is outlined in full within the ISA/IEC-62443-3-2 standard. The detailed risk assessment requires that a vulnerability assessment is conducted to identify unmitigated risk. These vulnerability assessments require that the assessment findings be qualitatively rated according to the threat, likelihood, and consequences should the vulnerability be exploited and threat actor success realized.

The IACS System Testing and Assessment Rating (STAR) Methodology (IACS STAR) is intended to be a methodology to estimate the severity of identified risks to the IACS/OT environment. This methodology includes the classic qualitative risk calculation elements while adding the consequence considerations necessary for understanding risks to IACS/OT processes and equipment. Having a system in place that addresses IACS/OT concerns for rating risks will save time and eliminate arguing about prioritizations and improve countermeasure selection to quickly reduce risk.

The authors of this methodology have tried hard to make this model simple to use, while keeping enough detail for accurate risk estimates to be made. The following resources help explain the challenges and obstacles for analyzing and rating risk in IACS/OT environments.

- The Blind Spot: How to Simply Calculate Cyber Attack Likelihood Using the Exploitability Assessment[2]
- Maximizing Limited Resources in OT Security - Spiceworks[3]

[1] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[2] https://www.cybersecureot.info/post/the-blind-spot-how-to-simply-calculate-cyber-attack-likelihood-using-the-exploitability-assessment
[3] https://www.spiceworks.com/tech/devops/guest-article/maximizing-limited-resources-in-ot-security/amp/

2.0 RISK ANALYSIS OVERVIEW

Over the years there has been a lot of debate about how to rate risk within industrial and automation control environments. Rating risk is difficult due to the varying ideas about likelihood, frequency, consequences, and impact ratings. This project is an effort to update the OWASP Risk Rating Methodology[4] to be usable when conducting security assessments and penetration tests within IACS/OT environments. It is not designed to replace a mature organization's risk rating methodology. It is intended for assessment teams to use when a specific methodology has not been defined or when a quicker method is needed to quickly rate and reduce risk.

For background, there are other more mature, popular, or well-established Risk Rating Methodologies that can be followed. Click the arrow for a list.

- ISA/IEC 62443 Series of Standards[5]
- NIST 800-30 - Guide for Conducting Risk Assessments[6]
- National Vulnerability Database (NVD) Common Vulnerability Scoring System Version 3 (CVSSv3) Calculator[7]
- Government of Canada - Harmonized TRA Methodology[8]
- Mozilla resources:
    - Risk Assessment Summary[9]
    - Rapid Risk Assessment (RRA)[10]

The risk and vulnerability assessment process is augmented by threat modeling to identify and prioritize potential attack vectors and successful exploitations.

The following is a list of methods to help with the threat modeling process.

- FIRST.org: Threat Modelling[11]
- The Operational Resilience Framework[12]
- Microsoft Threat Modeling Tool threats[13] - aka STRIDE
- MITRE's Threat Assessment and Remediation Analysis (TARA)[14]

[4] https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
[5] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[6] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[7] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
[8] https://cyber.gc.ca/en/guidance/harmonized-tra-methodology-tra-1
[9] https://infosec.mozilla.org/guidelines/assessing_security_risk
[10] https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html
[11] https://www.first.org/global/sigs/cti/curriculum/threat-modelling
[12] https://www.grf.org/orf
[13] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
[14] https://www.mitre.org/news-insights/publication/threat-assessment-and-remediation-analysis-tara

- ICS Layered Threat Modeling[15]
- OWASP Threat Modeling[16]
- OWASP Application Threat Modeling[17]
- OWASP pytm[18] - Pythonic framework for threat modeling
- OWASP Threat Dragon[19] - threat modeling tool

The ISA/IEC 62443 CSMS Detailed Risk Assessment process requires that considerations for the criticality of processes, equipment, and procedures are calculated and documented. Each process environment are unique to themselves. While the technologies and implementation details may be similar their implementation, management procedures, and selected countermeasures will be different for each instance. Indeed, the most effective way to secure these environments is to consider what the actual process is designed to accomplish and considering issues that might not necessarily be tied to common technological vulnerabilities that are evaluated by traditional risk and vulnerability assessment processes.

The following resources provide some details and insight into the considerations for this process.

- Idaho National Labs Cyber Informed Engineering[20]
- Idaho National Labs Consequence-driven Cyber-Informed Engineering[21]
- Critical infrastructure cybersecurity prioritization: A cross-sector methodology for ranking operational technology cyber scenarios and critical entities[22]
- Common Vulnerability Scoring System Version 4.0[23] - CVSS version 4.0 is the next generation of the Common Vulnerability Scoring System standard.

[15] https://sansorg.egnyte.com/dl/fztutwiK5J
[16] https://owasp.org/www-community/Threat_Modeling
[17] https://owasp.org/www-community/Application_Threat_Modeling
[18] https://owasp.org/www-project-pytm/
[19] https://owasp.org/www-project-threat-dragon/
[20] https://inl.gov/cie/
[21] https://inl.gov/cce/
[22] https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/critical-infrastructure-cybersecurity-prioritization/
[23] https://www.first.org/cvss/v4-0/

3.0 APPROACH

The ISA/IEC-62443-2-1 standard outlines that risk is calculated by taking the likelihood that an event will occur and scaling it with the consequences should the event be realized. Hence the equation ***Risk = Likelihood * Consequence***. The assignment of the likelihood and consequence variables is the typical debate.

Most IACS/OT likelihood calculations, sometimes referred to as frequency, take into consideration the commonly understood cases of equipment failure. Industrial and automation equipment have specific usage tolerances that, when calculated with known usage, can provide a measurable likelihood that the equipment will experience a problem. This often results in a likelihood table that uses specific timetables for an event to occur. A simple example could be:

- High: will occur in the next year
- Moderate: will occur in the next 10 years
- Low: no history of occurrence and therefore unlikely

These typical likelihood ratings are not applicable when considering cybersecurity and the likelihood or frequency that a threat actor will attempt to exploit a vulnerability. In 2008 the Federal Energy Regulatory Commission (FERC) determined that electric utilities required specific guidance to understand how to address likelihood and frequency when calculating risk. In FERC Order 706 Mandatory Reliability Standards for Critical Infrastructure Protection[24] the following guidance was provided:

- "Because there is insufficient data available to determine frequency, it should be assumed that an event will occur."
- "Risk-based assessment methodology should focus on the consequences of an outage, not the likelihood of an outage."

In the sections below, the factors that make up "likelihood" and "consequences" for IACS/OT environments are broken down as defined in the 'ISA/IEC-62443-3-2 Zone and Conduit Requirements (ZCR) 5: Perform a detailed cyber security risk assessment' section. The assessment team is shown how to leverage these factors to determine the overall severity for risks identified during a vulnerability assessment.

- Step 1: ZCR 5.1: Identify Threats
- Step 2: ZCR 5.2: Identify Vulnerabilities
- Step 3: ZCR 5.3: Factors for Estimating Consequences and Impact
- Step 4: ZCR 5.4: Factors for Estimating Likelihood
- Step 5: ZCR 5.5: Calculate Unmitigated Cybersecurity Risk
- Step 6: Reporting Vulnerabilities and Vector Scores
- Step 7: IACS STAR Calculator

[24] https://www.ferc.gov/sites/default/files/2020-04/E-2_11.pdf

3.1 Step 1: Identify Threats (ISA/IEC-62443-3-2 ZCR 5.1)

Following the model of the OWASP risk rating system there are a few factors that aid in the determination of risk. This effort has modified the OWASP model slightly to fit into the IACS/OT model. These factors are used when modeling attack scenarios to prioritize assessment efforts. The factors are also used when calculating the risk rating for each vulnerability and will vary according to the specifics of the situation. These factors include:

- a description of the threat actor group,
- the capabilities or skill-level of the threat actors,
- the possible motivations for the threat actors,
- the opportunities provided to the threat actors by the environment's architecture, and
- the level of access achieved when successfully exploiting the vulnerability.

3.1.1 Threat Actor Factors

It is important to understand threat actor groups when considering the skills, motivation, opportunities, and population of potential attackers. There are many lists that outline specific threat actor groups that are known to attack IACS/OT environments. These include Wikipedia: threat actor[25], MITRE[26], Mandiant[27], CrowdStrike[28], Dragos[29], and more. To perform vulnerability assessments there needs to be an easier list that allows all stakeholders to agree. Each of these groups are more accurately defined by their skills, likelihood of success, and primary objectives.

The following is one possible breakdown of threat actors associated with IACS/OT environments, each with their own levels of skill, motivation, opportunities, and group size.

- Malware: Malicious programs that have a specific effect on vulnerable / compromised systems. This includes general malware, IACS/OT malware, and custom malware.
- Script Kiddies: Uses tools, techniques, and malware that are known, common, and easily accessible.
- Cybercriminal: An advanced group that has the maturity and financial backing to obtain or develop tools, hire technology experts, and time to conduct research and development to achieve goals.
- Hacker: Individuals that are mainly comprised of security researchers and sensationalists. Their activities are typically limited to conducting vulnerability research

[25] https://en.wikipedia.org/wiki/Threat_actor
[26] https://attack.mitre.org/groups/
[27] https://www.mandiant.com/resources/insights/apt-groups
[28] https://www.crowdstrike.com/adversaries/
[29] https://www.dragos.com/threat-groups/

on products. Select individuals may progress to attempting to gain unauthorized access to understand risk and publicly disclose information.

- Competitor: Direct competitors with team members that will have access to specific knowledge that will apply in the case of specialized software and equipment.
- Employee: Disgruntled and reckless employees that have privileged access to systems and devices as well as knowledge about the technologies and networks.
- Vendor: Rogue vendor, integrator, or consultant that is disgruntled, reckless, or malicious. Have knowledge about technologies and may have privileged access to systems, networks, and devices.
- Cyberwarrior: Nation-state threat actors that typically operate in groups to achieve specific goals. Trained to live-off-the-land, steal credentials, and exfiltrate information. Has access to custom tools and malware designed to maintain persistence, propagate, and achieve their goals.

To compute the likelihood that a threat actor group will be successful the following numerical ratings will be assigned to skill level, motivation, opportunity, and size categories. The level of each category can be estimated to calculate the Threat Agent Factor which will be used to compute the overall likelihood that an event will be realized.

- Skill Level - How technically skilled is this group of threat actors?
    - Limited Information Technology (IT), network, and no Operational Technology (OT) skills (1)
    - Moderate IT, limited network, and no OT technical skills (3)
    - Advanced IT, moderate network, and limited OT technical skills (5)
    - Advanced IT, advanced network, and moderate OT technical skills (6)
    - Advanced OT technical skills (8)
    - Security penetration skills and knowledge of OT technologies (9)
- Motive - How motivated are the threat actors once they obtain access to the control environment? An excellent guide for this is the Impact column of the MITRE ATT&CK ICS Matrix[30].
    - No reward or intention to impact control environment (1)
    - Theft of operational data or equipment (2)
    - Create loss of view and control as a result of target-of-opportunity access to assets (3)
    - Limit access to fileshares and prevent view and control using common malware (5)
    - Prevent view and control using specially designed malware (6)
    - Manipulate view and control using privileged remote access and/or specially designed malware (8)
    - Prevent operation of safety equipment or cause a catastrophic failure (9)

[30] https://attack.mitre.org/matrices/ics/

- Opportunity - When accessing the control environment, how are the threat actors limited by deployed countermeasures?
    - Physical access and local authentication are required and response time is less than fifteen minutes (0)
    - Physical access and local authentication are required but response time is more than fifteen minutes (1)
    - Physical and remote access is possible, local authentication required, and active monitoring is enabled (3)
    - Limited logging of physical or remote access but administrative privileges are required to access network devices, systems, and applications (5)
    - Undetected physical or remote access but administrative privileges are required to access network devices, systems, and applications (6)
    - Undetected physical or remote access but requires authentication to some network devices, systems, and applications (8)
    - Undetected physical or remote access that provides elevated permissions to network devices, systems, and applications (9)
- Access - What are the physical or remote access capabilities achieved by successful exploitation within the process?
    - Physical owner/operator users (1)
    - Physical vendor / integrator users (2)
    - Physical non-malicious civilian users (4)
    - Remote owner/operator users (5)
    - Remote vendor / integrator users (7)
    - Physical malicious users (8)
    - Remote anonymous internet users (9)

3.2 Step 2: Identify Vulnerabilities (ISA/IEC-62443-3-2 ZCR 5.2)

The identification of vulnerabilities depends on the type of vulnerability assessment being conducted. Every IACS/OT environment will have a list of vulnerabilities that are a combination of known hardware and software vulnerabilities, configuration vulnerabilities, and technology implementation vulnerabilities. Some vulnerabilities can be identified using online research i.e., the NVD Vulnerabilities search page[31] and vendor cybersecurity resources pages. Configuration and implementation vulnerabilities are identified using passive and active vulnerability testing methods. The factors that play into rating identified vulnerabilities include:

- the ease of access,
- the ease of exploitation,
- public awareness of the vulnerability, and

[31] https://nvd.nist.gov/vuln/search

- detection and response of attempts to exploit the vulnerability.

3.2.1 Vulnerability Factors

The next set of factors are related to understanding the identified vulnerability. The goal here is to estimate the likelihood that the particular vulnerability will be exploited and used to gain access to the environment, provide persistence on a system or device, or be used to achieve the threat actor's goals. To understand the vulnerability the factors involving access, exploitation, and public awareness should be considered. Additionally, one of the Foundational Requirements outlined in the ISA/IEC 62443 series of standards includes Timely Response to Events (TRE). This should be added to the factors when understanding the vulnerability within the IACS/OT environment.

- Ease of Access - How easy is it for this group of threat agents to access the environment and discover the existence of the vulnerability?
    - Requires physical access to environment or OT device (1)
    - Requires physical access to environment or IT device (2)
    - Remotely accessible but countermeasures protecting OT technologies (3)
    - Remotely accessible but countermeasures protecting IT technologies (4)
    - Remotely accessible but no automated tools to discover for OT technologies (6)
    - Remotely accessible but no automated tools to discover for IT technologies (7)
    - Remotely accessible and automated tools available for IT technologies (8)
    - Remotely accessible and automated tools available for OT technologies (9)
- Ease of Exploit - How easy is it to actually exploit the vulnerability?
    - No known proof of concept (1)
    - Countermeasures protecting OT technologies (2)
    - Denial-of-Service possible but no code execution (3)
    - Custom scripts / tools can be made to exploit IT technologies (5)
    - Custom scripts / tools can be made to exploit OT technologies (6)
    - Automated tools available for IT technologies (8)
    - Automated tools available for OT technologies (9)
- Awareness - How well known is this vulnerability?
    - Unknown OT Vulnerability (1)
    - Unknown IT Vulnerability (2)
    - Not publicly known but common configuration vulnerability[32] (3)
    - Publicly identified on vendor website or within NVD Vulnerabilities database[33] but no known exploit available (5)
    - Publicly identified on vendor website or within NVD Vulnerabilities database[34] no known exploit available but target threat actor group can develop exploit (6)

[32] https://cwe.mitre.org/
[33] https://nvd.nist.gov/vuln/search
[34] https://nvd.nist.gov/vuln/search

    - Publicly identified on vendor website, vulnerability databases, and exploit available in public forums, e.g., Metasploit[35], Exploit-DB[36] (8)
    - Public identified and in CISA Known Exploited Vulnerabilities Catalog[37] (9)
- Detection/Response - How likely is an exploit to be detected?
    - Centrally logged with alerts and formal review and response plan (1)
    - Centrally logged with alerts and formal review but no response plan (3)
    - Centrally logged with alerts, but no formal review or response plan (6)
    - Centrally logged and without review (7)
    - Locally logged without review (8)
    - Not logged (9)

3.3 Step 3: Estimating Consequences and Impact (ISA/IEC-62443-3-2 ZCR 5.3)

The original OWASP risk rating methodology used a combination of technical and business impact factors to analyze the impact when a vulnerability's exploitation was realized. While useful these are not the best ways to understand the impact of an exploited vulnerability to an IACS/OT environment. The Impact column of the MITRE ATT&CK ICS Matrix[38] provides good details about what can happen after successful exploitation. These Impacts are a combination of denial, loss, and manipulation to the process or locations that monitor the process. The FIRST.org CVSSv4.0[39] scoring system has been updated to include a new supplemental metric group which includes rating factors that involve safety, automatable, recovery, value density, vulnerability response effort, and provider urgency. Hence, the IACS STAR will estimate consequences and impacts using technical factors and safety factors.

> NOTE: Business impacts are still an important factor for rating risk. However, business impact factors are considerations that should be left to the Detailed Risk Analysis. The IACS STAR is designed to be used when rating the risk of vulnerabilities which feed into the Detailed Risk Analysis process. Therefore, the IACS STAR calculations will attempt to understand the safety impact factors rather than the business impact factors. (Business impact factors may be incorporated into IACS STAR calculations at a future date.)

3.3.1 Technical Impact Factors

Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

[35] https://www.metasploit.com/
[36] https://www.exploit-db.com/
[37] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[38] https://attack.mitre.org/matrices/ics/
[39] https://www.first.org/cvss/v4-0/

- Loss of Confidentiality - How much data could be disclosed and how sensitive is it?
  - No data lost (0)
  - Minimal architecture configuration data disclosed (2)
  - Minimal network configuration data but no device configuration data disclosed (4)
  - Extensive network configuration data and some device configuration data disclosed (6)
  - Some process network and device configuration data disclosed (7)
  - All process network and device configuration data disclosed (9)
- Loss of Integrity - How is the process data changed and does it impact critical functions?
  - Modification of historical data not used for control (1)
  - Modification of historical data used for control (2)
  - Local modification of set points used for non-critical functions (4)
  - Remote modification of set points used for non-critical functions (5)
  - Remote modification of device configurations used for non-critical functions (6)
  - Local modification of set points used for critical functions (7)
  - Remote modification of set points used for critical functions (8)
  - Remote modification of device configurations used for critical functions (9)
- Loss of Availability - How are production and safety services impacted?
  - Minimal production interruption and easily recoverable (1)
  - Device or service interrupted but process not impacted (3)
  - Production services temporarily interrupted but easily recoverable (4)
  - Production services interrupted but does not affect other processes (6)
  - Production services interrupted and impacts other processes (7)
  - All production services completely lost (8)
  - Loss of process safety functionality (9)
- Loss of Accountability - Are the threat actor actions traceable to an individual?
  - Central logging, Multifactor Authentication (MFA), and cameras (1)
  - Central logging, Multifactor Authentication (MFA), but no cameras (2)
  - Local logging, Multifactor Authentication (MFA), and cameras but no central logging (3)
  - Local logging and cameras but no MFA and no central logging (5)
  - Local logging but no MFA, no central logging, and no cameras (7)
  - No local or central logging, no MFA, and no cameras (9)

3.3.2 Safety Impact Factors

The safety impact stems from the technical impact and requires a deep understanding of the process itself. The stakeholders of the System-Under-Consideration (SUC) will understand how each system and device within the SUC affects safe operations. These stakeholders will be able to provide details relating to how a situation, should exploitation of a condition be realized, will affect the environment, process, equipment, and issues related to recoverability.

Rating these factors takes a discussion between all team members. Initial ratings can be selected according to the information provided and conditions witnessed during the assessment. Selecting an initial rating will allow follow on discussions that will rate the factors more accurately.

- Environment Damage - How much damage to the local environment, plant or public, will be realized by successful exploitation?
    - No environmental impact (0)
    - Environment damage limited by safety equipment, active, and passive protections (1)
    - Environment damage limited by active and passive protections (2)
    - Environment damage limited by passive protections only (4)
    - Safety equipment not remotely accessible and active and passive protections are in place (5)
    - Safety equipment remotely accessible but active and passive protections are sufficient (7)
    - Safety equipment remotely accessible and situation might overwhelm active protections but passive protections are sufficient (8)
    - Safety equipment on production network and situation might overwhelm active or passive protections (9)
- Process Damage - How much damage to the process equipment will be realized by successful exploitation?
    - No devices can be damaged and configurations cannot be modified (0)
    - Device or monitoring systems / applications can be modified but do not damage device or process (1)
    - Device configuration can be changed but easily recoverable (3)
    - Device damaged requiring manual update but limited impact to process (4)
    - Device damaged requiring manual update and significant impact to process (6)
    - Safety equipment configuration changed but limited impact to process (7)
    - Safety equipment damaged but limited impact to process (8)
    - Safety equipment damaged causing process failure or automatic shutdown (9)
- Safety Equipment - How well is digital safety equipment deployed and protected?
    - Safety equipment not required for process (0)
    - Safety equipment required for process but not remotely accessible or on the same network as vulnerability (1)
    - Safety equipment required for process, remotely accessible, and requires MFA but not on the same network as vulnerability (2)
    - Safety equipment required for process and remotely accessible but does not require MFA and not on the same network as vulnerability (3)
    - Safety equipment required for process, remotely accessible, requires MFA, and on the same network as vulnerability (4)
    - Safety equipment required for process, remotely accessible, does not require MFA, and on the same network as vulnerability (5)

    - Safety equipment vulnerable and remotely accessible but requires MFA (6)
    - Safety equipment vulnerable and remotely accessible but requires authentication without MFA (7)
    - Safety equipment vulnerable and remotely accessible but requires authentication but default/hardcoded password in place and no MFA (8)
    - Safety equipment vulnerable, remotely accessible, and does not require authentication (9)
- Recoverability - How well is the organization / process team prepared to recover during successful exploitation?
    - Vulnerability will not require or limit recovery operations (0)
    - Process will automatically recover with no manual efforts (1)
    - Process will recover with minimal manual efforts (2)
    - Process will recover with extensive manual efforts (4)
    - Recovery not possible without vendor or integrator assistance (6)
    - Recovery not possible without limited government and vendor/integrator assistance (7)
    - Recovery not possible without moderate government and vendor/integrator assistance (8)
    - Recovery not possible without significant government and vendor/integrator assistance (9)

3.4 Step 4: Estimating Likelihood (ISA/IEC-62443-3-2 ZCR 5.4) and Consequences

The likelihood that the exploitation of a vulnerability will be realized is defined using the factors calculated when identifying threats and vulnerabilities. The scores of the threat and vulnerability factors, respectively, are added together and divided by the number of factors used in the calculation. The resulting values can then be assigned a less granular categorization (e.g., low, medium, and high) to limit subjectivity and improve consensus.

The same method will be used when calculating scores for consequences and impacts. The scores for the technical and safety impacts will be combined to achieve a low, medium, or high categorization. To calculate the likelihood and consequences rating category the 0 to 9 scale is split into three parts:

Scoring Categories	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

3.5 Step 5: Calculate Unmitigated Cybersecurity Risk (ISA/IEC-62443-3-2 ZCR 5.5)

Once the likelihood and consequence ratings have been determined the overall risk associated with the vulnerability can be calculated. This calculation will result in the unmitigated risk rating for the vulnerability which is required for input into the ISA/IEC 62443 Detailed Risk Analysis. The following table will be used to combine the resulting likelihood and consequence categories and assign an unmitigated risk score.

Unmitigated Risk Score				
Consequences	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Informational	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

3.6 Step 6: Reporting Vulnerabilities and Vector Scores

The assessment report is the most important part of an assessment. It provides context about the scope of the assessment, the assets involved, the communications between assets and across enforcement boundaries, the methodology used to gather information, details about the findings, and the vulnerability scores for these findings. The report should be clearly written to convey all this information and the results should be reviewed by all stakeholders. Eventually the information from the assessment will be used in a Detailed Risk Assessment. To this end, like the OWASP risk rating methodology, the IACS STAR scores can be categorized using a vector

score. This vector score provides the likelihood and consequence factor scores when rating the risk. This allows easy integration with most automated risk and vulnerability management systems and scoring calculators. To aid the generation of a vector score each of the factors have been provided an identifier.

- Skill Level (SL)
- Motive (M)
- Opportunity (O)
- Access (A)
- Ease of Access (EA)
- Ease of Exploit (EE)
- Awareness (AW)
- Detection/Response (DR)
- Loss of Confidentiality (LC)
- Loss of Integrity (LI)
- Loss of Availability (LA)
- Loss of Accountability (LAC)
- Environmental Damage (ED)
- Process Damage (PD)
- Safety Equipment (SE)
- Recoverability (R)

Once computed the resulting score vector would be represented in the following format:

(SL:0/M:0/O:0/A:0/EA:0/EE:0/AW:0/DR:0/LC:0/LI:0/LA:0/LAC:0/ED:0/PD:0/SE:0/R:0)

4.0 IACS STAR CALCULATOR

The IACS STAR score calculator (website coming soon) has been set up to aid in the calculation of the IACS STAR vulnerability scores. This calculator follows the model provided by the OWASP Risk Rating Calculator[40]. It can be used when considering the scoring of each of the factors that are used to calculate likelihood and consequence. It is intended to aid in discussions and to move towards consensus amongst stakeholders. It can also be used to provide the vector score to be added to the assessment findings.

4.1 Online IACS-STAR Calculator

- The online calculator: https://iacs-star-calculator.com
- The online documentation: https://iacs-star-calculator.com/methodology.html

4.2 On Premises IACS-STAR Calculator

To run this calculator locally clone this repository, open a terminal to the repo directory, and run a Python web server with the following command:

```
python3 -m http.server 9000
```

Open your web browser to your local IACS STAR score calculator at http://localhost:9000/iacs_star_calculator.html.

[40] https://owasp-risk-rating.com/