Cyber Resilience Metrics Assesment Report



**CRMETRICS**

# Report for {{company}} – {{survey}}

Date of Creation: {{date}}

**Disclaimer**

The analysis, data, and reports are provided “as is” for informational purposes only. Use of this tool and report does not provide any warranties of any kind regarding any information contained within.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact RF. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of RF.

Few things to note about this document:

* This document is a point-in-time document prepared after CR Metrics assessment and may not represent the actual or current posture of resilience of assessed entity.
* The document was prepared for internal assessment to derive a high-level cyber resilience indicator of assessed entity using the current version of CR Metrics tool, but not an exhaustive assessment of resilience indicators and does not claim to represent an accurate picture of entities CR posture.
* This document is provided as “for information only” to entities to make them aware of cyber resilience indicators and should not be taken as a directive to take specific actions or as our advice on how to approach mitigation/compliance.

Table of Contents

[Report for {{company}} – {{survey}} 1](#_Toc11962944)

[Introduction/Methodology 4](#_Toc11962945)

[1. Resilience Metrics Summary 6](#_Toc11962946)

[1.1. Robustness Metric 6](#_Toc11962947)

[1.2. Redundancy 7](#_Toc11962948)

[1.3. Resourcefulness 8](#_Toc11962949)

[1.4. Rapidity 9](#_Toc11962950)

[2. Areas needing attention 10](#_Toc11962951)

[3. Recommendations 11](#_Toc11962952)

[REFERENCE 19](#_Toc11962969)

# Introduction/Methodology

The National Academy of Science defines resilience as the ability of a system to plan/prepare, absorb, recover and adapt [1]. The Plan/Prepare aspect focuses on keeping services available and assets functioning during a malfunction or attack. The Absorb aspect is to continue to function during an attack and repel or isolate the attack. The Recover aspect is to get back all functions and services to pre-attack levels and Adapt aspect is to utilize the knowledge and experience gained to become more resilient.

The National Institute of Standards and Technology (NIST) provides a framework for improving the cybersecurity and resilience of critical infrastructures that are supported by both Information Technology Systems and Industrial Control System. The NIST framework identifies five functions that organize cybersecurity at the highest levels: Identify, Protect, Detect, Respond and Restore [2]. The Identify aspect focusses on to develop an understanding of and manage risk to systems, assets, data, and capabilities. The Protect aspect focusses to develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The Detect aspect identifies the occurrence of a cybersecurity event. The Respond aspect focuses to take action regarding a detected cybersecurity event and recover aspect focus on maintaining plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Increasing resilience in Energy Critical infrastructure systems improves overall infrastructure’s functionality and performance. Researchers at Multidisciplinary Center for Earthquake Engineering Research (MCEER), sponsored by the National Science Foundation and headquartered at the University at Buffalo developed the R4 framework of resilience [3].

- Robustness: The ability of systems, system elements, and other units of analysis to withstand disaster forces without significant degradation or loss of performance

- Redundancy: The extent to which systems, system elements, or other units are substitutable, that is, capable of satisfying functional requirements, if significant degradation or loss of functionality occurs

- Resourcefulness: The ability to diagnose and prioritize problems and to initiate solutions by identifying and mobilizing material, monetary, informational, technological, and human resources;

- Rapidity: The capacity to restore functionality in a timely way containing losses and avoiding disruptions.

In this methodology of deriving cyber resilience metrics, we adopted a set of comprehensive security metrics from the R4 resilience framework that can effectively measure cyber resilience across the bulk power system (BPS) network. We think the R4 resilience framework [3] is a good fit for the bulk power system cyber resilience analysis because the R4 metrics (Robustness, Redundancy, Resourcefulness, and Rapidity) cover the functions required to be a resilient BPS as identified by NIST framework [4, 5], where we consider BPS as a critical infrastructure. We further decompose the four R4 metrics into a hierarchy of several more easily comprehended sub-metrics, each of which can be analyzed independently. The sub-metrics are organized to capture qualitative information about the system’s security and can serve as a high-level management tool to identify where analysis and modeling should be carried out. While designing the questionnaires sets to collect the qualitative information related to the bulk power system network, we follow NIST bulk power system security guidelines [5-7] and ICS-CERT industrial control systems (ICS) standards [6] and other scholarly articles [8]. Because resilience depends on the effective functioning of all aspects of the bulk power system, the framework must consider the physical domain, the organizational practices, and the technologies implemented in the system. Thus, our framework is categorized into three notional layers: physical, organizational, and technological. Through these notional layers and subcategories, cyber resilience metrics are derived to present the indicators of performance and gain an understanding on aspects contributing to resilience.

The sub-metrics are scored from 1.0 to 5.0 based on the user inputs on a Likert scale. The metrics or sub-metrics that are within the range of 4.6 to 5.0 are treated as “Excellent”, means the organization is performing excellently in securing those areas from cyber resilience perspectives. The sub-metrics that have values between 3.6 to 4.5 are treated to be “Very Good”, means the organization’s standings on those areas are very good. Similarly, the metrics having scores between 2.6 and 3.5 are treated as “Good”, means the organization’s performances on those areas are good and there are scopes for improvement in the current organizational setup and practices to secure the bulk power system network by analyzing the underlying sub-metrics. The metrics having scores between 1.6 to 2.5 are treated as “Fair”, means those areas are doing somehow ok, but there are needs for improvement. The metrics having scores of 1.0 to 1.5 are treated as “Poor”, means that the organization is performing poorly on those areas and the management needs to focus on those areas which are performing poorly comparing to the other areas in terms of cyber security of the overall bulk power system network.

# Resilience Metrics Summary

The cyber resilience metrics are assessed using the R4 framework across the three physical, organizational and technological dimensions. The assessment has been conducted based on the responses provided by ***{{number}}*** individuals. This section provides the graphical view of the overall summary of the responses for each of the R4 framework components.

{{p complete}}

Figure 1.Overall Resilience Metrics Summary

## Robustness Metric

The below figure illustrates the robustness metric for the three dimensions (physical, organizational and technical). In each dimension, robustness is decomposed into several sub metrics each of which can be analyzed independently Each row represents the labeled sub metric score so that the combined average gives the corresponding robustness in that dimension.

{{p bar1}}

Figure 2. Dimensional Robustness Metrics Bar Chart

Place holder For Dynamic Data

{{p radar1}}

Figure 3. Robustness Sub-Metrics

Place holder For Dynamic Data

## Redundancy

The below figure illustrates the redundancy metric is for the three dimensions (physical, organizational and technical). In each dimension, redundancy is decomposed into several sub metrics each of which can be analyzed independently Each row represents the labeled sub metric score so that the combined average gives the corresponding redunadancy in that dimension.

{{p bar2}}

Figure 4. Dimensional Redundance Metrics Bar Chart

Place holder For Dynamic Data

{{p radar2}}

Figure 5. Redundancy Sub-Metrics

Place holder For Dynamic Data

## Resourcefulness

The below figure illustrates how the resourcefulness metric is evaluated for the three dimensions (physical, organizational and technical). In each dimension, resourcefulness is decomposed into several sub metrics each of which can be analyzed independently Each row represents the labeled sub metric score so that the combined average gives the corresponding resourcefulness in that dimension.

{{p bar3}}

Figure 6. Dimensional Resourcefulness Metrics Bar Chart

Place holder For Dynamic Data

{{p radar3}}

Figure 7. Resourcefulness Sub-Metrics

Place holder For Dynamic Data

## Rapidity

The below figure illustrates the rapidity metric for the three dimensions (physical, organizational and technical). In each dimension, rapidity is decomposed into several sub metrics each of which can be analyzed independently Each row represents the labeled sub metric score so that the combined average gives the corresponding rapidity in that dimension.

{{p bar4}}

Figure 8. Dimensional Rapidity Metrics Bar Chart

Place holder For Dynamic Data

{{p radar4}}

Figure 9. Rapidity Sub-Metrics

Place holder For Dynamic Data

# Areas needing attention

The above chart shows performance of each subject area. Each bar represents the labeled subcategory and its contribution in the resilience score. Physical diversity, Technical composition and Technical network communication are the areas that need most attention. Below are recommendations to improve overall resilience

* Employing devices from diverse ICS vendors will increase the difficulty of cyber-attacks and make the system more resilient. The diverse devices cannot be targeted easily by the same attack vector.
* There should be sufficient variety in the type of devicess in use over time, thus creating an element of surprise and difficulty for a potential attacker
* The secondary or backup assets (such as computers, software, applications, etc.) should be diverse to ensure they are not susceptible to the same vulnerabilities as their primary counterpart.
* Use diverse cyber products (router/firewall hardware and software, computer hardware and operating systems) If same product is used, they will all share the same vulnerabilities. if the attacker compromises the first firewall, he/she will then have the knowledge to compromise the subsequent firewalls in the attack path.
* Standard redundancy may not be sufficient since the redundant item may still have the same vulnerability as the primary. Organizations need to compose new protocols, software's and configurations that are interoperable with the system and can resist to previous cyber-attacks to ensure continuity of service
* Deploy defined alternate protocols/software's to support your service. For example, an organization should be able to switch from IP v4 to IP v6
* Employ dynamic defense techniques, such as, moving target defense to improve resilience to APT
* Provide extended processing and memory capacities to your ICS components to run both ICS applications and computationally expensive security mechanism. Several ICS components were designed a long time ago, with low memory and CPU capacities. As a consequence, a lot of ICS modules may respond slowly, especially when they execute cryptographic security modules that require large memory/CPU consumption.
* Design communication network in accordance with the specifications of protocol standards such as IEC 61850 defining communications for SCADA systems For example, the control center could be separated from RTUs by thousands of miles, and as a result, latency, bandwidth, jitter and reliability of the communication channel may influence the ability to operate in real time.

{{p chart5}}

Figure 10. Areas doing well and areas needing attention

# Recommendations

Generic submetrics level recommendations are provided below with reference to the the standards and scholarly articles.

### Robustness:

### Physical Robustness:

* **Physical Access Control:**

1. Implement standard physical security mechanisms (e.g., smart card, PIN etc.) to allow access into the SCADA control centers, ICS devices switch rooms, and field locations.
2. Use multi-factor authentication to the SCADA, ICS, or field devices. An example could be a combination of password along with an instantly generated security token from a secure device (e.g, RSA token) or a combination of password and user PIN (personal identification number), or smart card and password.
3. Always use separate secured rooms and secured racks to install the ICS or field devices. This means place the ICS or field devices in a separate secure place where access to them is controlled by security control mechanisms such as smart cards (e.g., employee chip-enabled ID cards).
4. Prohibit unauthorized devices (any personal device which is not provided by the authorized personal of the organization) in the field locations or sites (i.e., switch rooms) where the ICS devices are located. Allow use of only authorized devices which are pre-screened by the security experts.

**Reference: [4, 9, 10]**

* **Diversity:**

1. Use multiple vendors for selecting the ICS hardware and software. Do not use only one vendor in the ICS systems, because this gives the attacker the privilege to breach multiple system components by being able to compromise the security of a single device because of the same vulnerability.
2. Use diverse product combinations in your IT network, an example could be a mix of Windows computer along with Apple computers, or a mix of Linux based computer and windows-based computers.
3. Use diverse software applications to access to the ICS devices. An example could be control computer (HMI) that is installed with Siemens proprietary software to access Siemens PLC should not install any other vendor’s (e.g., Rockwell Automation) proprietary software to access to the other PLC (Rockwell PLC).
4. Allow randomness to vary the type of the devices in use over time. For example, if the physical security is controlled by a combination of smart card and pin for long term (6 months-1 year), then change to access control mechanisms to any other combinations (such as biometrics and RSA security token).

**Reference: [11, 12]**

### Organizational Robustness:

* **Role-based Access Control:**

1. Always use least privilege principles, i.e., allow access only to the information or resources that are necessary for accomplishing the assigned tasks by the employee.
2. Prohibit direct local or remote access to critical system by the industry partners or 3rd party users.
3. Always follow the proper approval process to create new user accounts for the system users and keep record of any change in the user account systems.

**Reference: [13-15]**

* **Audit and Accountability:**

1. Conduct periodic (at least once in 3 months) security trainings to familiar the employees with the system use policies and standards, recent malicious attacks on similar systems etc.
2. Arrange security exercises to increase the cyber awareness among the employees. This includes controlled penetration tests, identification of malicious activity etc.
3. Circulate the system use policy guidelines to the employees and users of the system and keep them updated frequently if any change in the policy is done which the users may not be aware of.

**Reference: [4, 14-16]**

* **Insider Threat Management:**

1. Include the insider threat awareness into the periodic security training programs
2. Articulate the organizations policy to handle the insider threat and explain which activities may lead to suspect someone as part of insider threat vector (such as communicating or spreading of system sensitive information to an outsider using the company email address).
3. Always maintain event management system to audit users’ actions. An example could be, monitor the command logs and make an alert system to automatically generate alarms when any system critical command is given from any user workstation.

**Reference: [17]**

### Technical Robustness:

* **ICS Weakness:**

1. Follow the vendor recommendations and standards (NIST, NERC-CIP) for your SCADA computers, servers, ICS devices, and other critical assets.
2. Frequently update the latest patch on the control system computers.
3. If there is any anomaly detected in the PLC level, consult with the vendor for possible solutions or patches.

**Reference: [18]**

* **Segmentation and Segregation:**

1. Apply network segmentation by segregating the sensitive OT devices from the other IT devices.
2. Place the servers that communicate with ICS devices in a separate DMZ and restrict access of those servers from the corporate network using firewalls.
3. Frequently check/update the firewall settings or ruleset so that it conforms to the network design and there is no traffic or message communications between the network components that are not allowed in the design or network topology.
4. Use private VLANs to protect networks from unwanted traffic from untrustworthy devices.

**Reference: [19]**

* **Diversity:**

1. Use diverse products from different vendors for the IT network.
2. Consider using different vendors for similar type of products for example different firewalls or routers from different vendors. Choose from a list of preferred vendors whose systems are reported as less vulnerable and hard to penetrate.
3. Use DMZ between control and corporate network and restrict message or traffic communication from DMZ towards control network unless extremely necessary.

**Reference: [12, 19]**

* **Logical Access Control:**

1. Make sure the authentication process is encrypted and supported by encryption mechanisms.
2. Make sure all the web communication is on secure HTTPS, not on HTTP. Make sure the certificate is updated and the signature is verified.
3. Use VPN (Virtual Private Network) to communicate with the ICS network from outside especially for remote access by 3rd party or business partners.
4. Create and apply Layer 2 (L2) access control lists (ACLs) and Virtual ACLs, blocking the direct com­munication at L2 between a potential attacker and the attacked device.

**Reference: [9, 14, 19]**

### Redundancy:

### Physical Redundancy

* **Devices:**

1. Use backup devices as secondary source for continuation of service. In case the primary devices are under adverse events because of any cyberattack, then the secondary devices can keep the services and functionality running without any loss.
2. Always apply redundancy in switches, routers, firewalls, and ports.
3. Make sure that the ICS devices and control room servers have uninterruptible power supply (UPS).
4. Consider placing the secondary devices in geographically diverse location rather than putting everything in one site. Incase the site is unavailable or if the cyber attacker is able to take the primary site out of service by being able to make a cascading failure on the primary site, then the functionality and services should switch to the secondary devices in the secondary site. This can be applied only to the critical assets if the budged and cost is a concern.

**Reference: [10, 20, 21]**

* **Network:**

1. While designing the network topology or architecture, always consider the redundancy in equipment or node level as well as the link and port levels to avoid single point of failure.
2. Always maintain proper cable labeling and design documents readily available on site for any emergency handling (e.g., a physical cable may need to remove from specific ports to isolate the attack and to stop the attack propagation).

**Reference: [9, 10, 19]**

* **Process:**

1. Establish defined processes and directions to follow in case of any adverse events.
2. Consider having backup process plans to execute incase the primary restoration plan or process is not working.

**Reference: [10]**

* **Supply:**

1. Always make sure there is an alternate source of power supply is available incase the primary power source is taken out of service by some adverse events.
2. Implement backup or redundant physical links towards the routers, switches to ensure uninterrupted connections.

**Reference: [14, 19]**

### Organizational Redundancy:

* **Change Management Policy:**

1. Evaluate all the network change requests or update requests before implementing and follow organizational approval process.
2. Always test in offline mode (testbed mode or in low usage hours) any changes needed to be done in the configuration of the system or service, so that the impact is minimal.
3. Consult with the vendors of the assets before any major change is implemented.
4. Document all the changes and impacts or consequences faced for post-reviews.

**Reference: [14, 22]**

* **Site Contingency:**

1. Site contingency is needed to be considered to avoid the cascading failures.
2. Alternate sites should be fully operational and maintained regularly.
3. Considering the cost of operation and maintenance of secondary sites, only the critical service assets may be placed in the secondary sites to ensure the continuity of services.
4. Consider implementing load sharing towards the healthy sites, incase if the secondary site is not used. Thus, plan the capacity accordingly so that incase of adverse event, there are enough capacity in the healthy sites to forward the traffic or services from affected sites.

**Reference: [19]**

* **Insider Threat Management**

1. Implement knowledge sharing among the closely operated IT/OT engineers and operators. Thus, an employee may not be expert in all domains, but if he or she can perform the emergency tasks needed to be carried out, then absence or dismissal of any employee would not affect the service or operation continuity.

**Reference: [4, 15, 16]**

### Technical Redundancy:

* **Information System Backup:**

1. Always backup your core network systems data and information and keep them in a secure place easily accessible in case of emergency.
2. Consider implementing secondary backup systems for the critical data
3. Consider testing the backup files by examining the restoration process in offline mode or low usage hours (e.g., at mid-night 2AM to 3AM).

**Reference: [14]**

* **Composition:**

1. Consider implementing Software defined network (SDN) switches to facilitate automatic reconfiguration of network topologies incase the service is impacted which facilitates minimum human intervention.
2. Consider implementing software modules capable of inter operating successfully with different protocols and different message communications.

**Reference: [22]**

### Resourcefulness:

### Physical Resourcefulness:

* **Monitoring and Detection:**
  1. Always deploy access monitoring systems which include video cameras, sensors, and other types of identification systems to monitor the technical infrastructure including control rooms and switch rooms. Provide adequate lighting based on the type of monitoring devices deployed.
  2. Deploy asset location tracking technologies which can track the movements of people and vehicles with the plant to ensure that they stay in authorized areas, identify personnel needing assistance, and support emergency response.
  3. Deploy asset management systems which keeps logs of faulty system devices that are replaced by new hardware or software to quickly identify any changes in the networked system.
  4. Make sure computers and computerized devices used for ICS functions never leave the control or switch room area. Laptops, portable engineering workstations, and handhelds should be tightly secured and never used outside the ICS network.
  5. Deploy routine check to the sensors and actuator devices in the field stations if they have any LED indicating malfunction of the device or need a reset. Routine physical check may also apply to other critical assets.

**Reference: [14, 23]**

* **Response and Recovery:**

1. Make sure a security monitoring team is available 24x7x365 to monitor and analyse any security breach to the IT network, substations, plants, and ICS control rooms.
2. Allow remote analysis and restoration of the ICS or SCADA system incase of on-site support is not available.
3. It is recommended to have a field support team who are available during any adverse events to support on-site.
4. Update the event management systems with the procedure if any cyber compromise is detected and mitigated, so the learning can be used in future for the similar scenario.

**Reference: [19, 23]**

### Organizational Resourcefulness

* + **Monitoring and Detection:**

1. Setup established monitoring and detection plans and procedures consulting with the OT (ICS, SCADA) experts, IT experts, technical managers, vendors, regulatory bodies and other stakeholders of the system.
2. Make sure you have plans and procedures for regular system audits.
3. Perfom periodic audit for system vulnerability and make sure the system patches are updated as per vendor recommendations.

**Reference: [10, 19, 23]**

* + **Response and Recovery:**

1. Setup response and recovery plans and procedure to follow incase of system downgraded performances due to cyber events.
2. Always record and categorize cyber incidents based on their type, time and duration of attack, impact and recover methods etc.
3. Circulate the response and recovery plan to respective section of the employee and train them to learn the outcome.

**Reference: [10, 23]**

* + **Resilient Management:**

1. Setup a practice to communicate the procedures to follow for maintaining resilient system to the top-level management as this may involve cost and need to consult the budgetary restrictions.
2. Develop accurate response actions by consulting cyber incidents occurred in the ICS system and correlating them to the guidelines and standards provided by the regulatory bodies or any other public databases (for example, NVD).

**Reference: [23]**

* + **Communication:**

1. Disseminate standard security practices to all level of employess operating in the IT and OT domain.
2. Involve internal parties (i.e., support team, emergency response team, business units, and managements) and external parties (i.e., vendor contacts, ISP, regulatory agencies etc.) and other stakeholders in developing an effective response and recovery plan for the ICS and IT systems.

**Reference: [23, 24]**

* + **Insider Threat Management:**

1. Include the insider threat management policies into the organizational information and data security policies.
2. Train operators and technical staffs regarding the organization’s information security policies.

**Reference: [4, 14-16]**

### Technical Resourcefulness

* **Monitoring and Detection:**

1. Deploy intrusion detection systems (IDS) that is capable of monitrong and create alarms for any abnormal traffic operation in the ICS environments. Make sure the IDS rulesets are written to monitor for IP sources and destinations, protocols, lengths of packets, and traffic signatures provided by ICS vendors for their equipment.
2. Deploy monitoring system that can monitor the usage of IT services and ICS functionalities. ICS functionality monitoring would allow to observe the system usages and identify any breakdown of processes or any loss of services or other abnormal system behavior such as high CPU load, unusual traffic volume etc.
3. Enable event and command logging on firewalls, servers, monitoring system, and SCADA computers or workstations. This allows logging of consecutive invalid login attempts, any attempt to clear the log files, unauthorized patch loading, unexpected shutdown of the system etc.
4. Enable automatic security alerts where possible. This may include security alerts for certain number of failed attempts to login to SCADA computers or any other human machine interfaces (HMI) including the IT network computers.

**Reference: [12, 19]**

* **Response and Recovery:**

1. Consider deploying Intrusion Prevention Systems (IPS). Make sure the IPS solutions are in-line with the firewalls and compatible with the ICS equipment and can act by blocking traffic that does not meet the defined rules.
2. Make sure the login system rulesets of the ICS controlling computers are such that it can lock the account for centrain consecutive invalid attempts or terminate sessions for certain period of inactivity.
3. Make sure that the emergency technical support system or regular operational support system are consisted with engineers and experts to be able to analyse any threats, abnormal traffic behaviors, initiate traffic isolation and system restoration. Make sure that the support is available 24x7x365 and both on-site and remotely.

**Reference: [4, 10, 23]**

### Rapidity:

### Physical Rapidity:

* + **Accessibility:**

1. Ensure that there are adequate backup supply hardware or devices available and easily accessible in case of necessary emergency replacement.
2. Practice using warehouse located in every plant location which consists of backup supply of hardware, software and other toolkits and are easily accessible by the emergency response team or support team.
3. Practise documenting emergency instructions and make them readily accessible in all control rooms or plant locations.

**Reference: [23, 25]**

### Organizational Rapidity:

* + **Emergency Management:**

1. Train the technical staffs regarding emergency handling and recovery procedures.
2. Communicate any emergency action plan to the other associated parties (vendors, customers, and suppliers).
3. Always document and keep log of the actions performed during emergency handling so that it can be used for future learning and continuous improvements.

**Reference: [4, 13-15]**

* + **Awareness and Training:**

1. Organize trainings to aware internal parties such as employees, technical staffs, managers about their roles and responsibilities to perform during an emergency event. This would help them to take quick actions in emergency.
2. Organize sessions with other stakeholders to aware them regarding organization’s cyber security policies.
3. Setup simulation environments to practice penetration test and other security exercises.

**Reference: [4, 14-16]**

* + **Insider Threat Management**

Organizations should be able to identify any insider threat vector so that the insider threat may not be able to cause any harm to the system.

1. Train employees, technical staffs, operators, and managers about social engineering (such as Phishing, Pretexting, tailgating etc.). Train the staffs regarding the common practices to avoid social engineering scams.
2. Train staffs regarding recognizing and reporting potential indicators of insider threat to the concerned bodies. Common symptoms to identify insider threats are attempts to gain access to unauthorized information out of scope of work, any intentional violations of organizational policies, degraded job-performances etc.
3. Develop a practice to engage all the employees of the organizations to think as part of the organization. Team building efforts may help in this regard.

**Reference: [16, 23]**

### Technical Rapidity:

* **Processing:**

1. Ensure the technical staffs know the decision-making process to rapidly act when an intrusion is detected.
2. Ensure the intrusion detection system (IDS) and intrusion prevention system (IPS) can detect and quarantine accurately any intrusion incident without human interactions. IDS and IPS should be able to automatically isolate the affected part of the system from the network to stop the propagation of the malware.
3. Consider upgrading your ICS devices and applications.

**Reference: [14, 23]**

* **Network level communication:**

1. Ensure the network communication follows the specifications of the protocol standards (i.e. IEC 61850) for ICS or Secure SCADA Communications Protocol (SSCP) for SCADA communication.
2. Allow only authorized remote access to the ICS and SCADA systems to quick analysis and recovery of the system incase of adverse events.

**Reference: [19, 26]**

* **Configuration:**

1. Ensure the system backup informations are readily available for emergency restoration process.
2. Ensure the switching to the backup source or system has no impact on the continuity of services.
3. Ensure that the system configuration changes can be done within the acceptable recovery time during a disruption of service events.

**Reference: [22, 23]**

# REFERENCE

[1] S. L. Cutter, J. A. Ahearn, B. Amadei, P. Crawford, E. A. Eide, G. E. Galloway, M. F. Goodchild, H. C. Kunreuther, M. Li-Vollmer, and M. Schoch-Spana, “Disaster resilience: A national imperative,” *Environment: Science and Policy for Sustainable Development,* vol. 55, no. 2, pp. 25-29, 2013.

[2] A. Sedgewick, *Framework for improving critical infrastructure cybersecurity, version 1.0*, 2014.

[3] K. Tierney, and M. Bruneau, “Conceptualizing and measuring resilience: A key to disaster loss reduction,” *TR news*, no. 250, 2007.

[4] NIST. "Framework for Improving Critical Infrastructure Cybersecurity," <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

[5] K. Stouffer, J. Falco, and K. Scarfone, “Guide to industrial control systems (ICS) security,” *NIST special publication,* vol. 800, no. 82, pp. 16-16, 2011.

[6] ICS-CERT, "Industrial Control Systems Standards and References."

[7] K. Stouffer, and J. Falco, "Guide to supervisory control and data acquisition (SCADA) and industrial control systems security," National institute of standards and technology, 2006.

[8] R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, “On the definition of cyber-physical resilience in power systems,” *Renewable and Sustainable Energy Reviews,* vol. 58, pp. 1060-1069, 2016.

[9] NCCIC. "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," <https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf>.

[10] US-CERT. "Cyber Resilience Review (CRR) Supplemental Resource Guide, Volume 1, Asset Management," <https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM.pdf>.

[11] MITRE. "Cyber Resiliency Engineering Framework," <https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework>.

[12] MITRE. "Cyber Resilience for Mission Assurance," <https://ieeexplore.ieee.org/iel5/6095473/6107829/06107877.pdf>.

[13] ISO/IEC27001:2013. "Information technology -- Security techniques -- Information security management systems -- Requirements," <https://www.iso.org/standard/54534.html>.

[14] N. SP800-53. "Security and Privacy Controls for Information Systems and Organizations " SP 800-53; <https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf>.

[15] CIS. "Critical Security Control V7," <https://www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/>.

[16] US-CERT. "Cyber Resilience Review Supplemental Resource Guide, Volume 9, Training and Awareness," <https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-TA.pdf>.

[17] NITTF. "Insider Threat Guide: A compendium of best practices to accompany the national insider threat minimum standards," <https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf>.

[18] E. J. M. Colbert, and A. Kott, *Cyber-security of SCADA and Other Industrial Control Systems*.

[19] N. SP800-82. "Guide to Industrial Control Systems (ICS) Security," <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf>.

[20] R. Albert, I. Albert, and G. L. Nakarado, “Structural vulnerability of the North American power grid,” *Physical review E,* vol. 69, no. 2, pp. 025103, 2004.

[21] A. Chaves, M. Rice, S. Dunlap, and J. Pecarina, “Improving the cyber resilience of industrial control systems,” *International Journal of Critical Infrastructure Protection,* vol. 17, pp. 30-48, 2017.

[22] US-CERT. "Cyber Resilience Review (CRR) Supplemental Resource Guide, Volume 3, Configuration and Change Management," <https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-CCM.pdf>.

[23] US-CERT. "Cyber Resilience Review Supplemental Resource Guide, Volume 5, Incident Management," <https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf>.

[24] NIST. "Special Publication 800-61," <https://csrc.nist.gov/publications/detail/sp/800-61/archive/2004-01-16>.

[25] P. W. Parfomak. "Congressional Research Service - Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations," <https://fas.org/sgp/crs/homesec/R43604.pdf>.

[26] D. DHS. "Energy Sector-Specific Plan," <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2010-508.pdf>.