Cyber Security Risk Mitigation Checklist

Contents

- Building a Risk Management Program
- Cyber Security Policy
- Personnel and Training
- Operational Risks
- Insecure SDLC Risks
- Physical Security Risks
- Third Party Relationship Risks
- Network Risks
- Platform Risks
- Application Layer Risks
- AMI
- MDM
- Communication Systems Scada
- In Home Displays
- Web Portals
- DR over AMI
- Interactive Thermal Storage
- Advanced Volt / VAR
- Conservation Voltage Reduction

Building a Risk Management Program (1)

Activity / Security Control	Rationale
Provide active executive sponsorship	Active and visible support from executive management at each stage of planning, deploying, and monitoring security efforts is crucial to success.
Assign responsibility for security risk management to a senior manager	Have security risk mitigation, resource-allocation decisions, and policy enforcement roll up to a clearly defined and executive with the requisite authority.
Define the system	Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security.
Identify and classify critical cyber assets	It is important to understand the assets that may need to be protected along with their classification (e.g., confidential information, private information, etc.) That way an informed decision can be made as to the controls needed to protect these assets that are commensurate with risk severity and impact to the business.
Identify and document the electronic security perimeter(s)	It is important to understand the entry points into the organization that an adversary may use as a starting point for going after the assets in order to build a threat model. The threat model than becomes an important component of the risk assessment.

Building a Risk Management Program (2)

Activity / Security Control	Rationale
Identify and document the electronic security perimeter(s)	It is important to understand the entry points into the organization that an adversary may use as a starting point for going after the assets in order to build a threat model. The threat model than becomes an important component of the risk assessment.
Perform a vulnerability assessment	Realistic assessments of (a) weaknesses in existing security controls and (b) threats and their capabilities create the basis for estimating the likelihood of successful attacks. They also help to prioritize remedial actions.
Assess risks to system information and assets	The risk assessment combines the likelihood of a successful attack with its assessed potential impact on the organization's mission and goals. It helps ensure that mitigation efforts target the highest security risks and select controls that are appropriate and cost-effective for the organization.
Select security controls	Appropriate management, operational, and technical controls cost-effectively strengthen defenses and lower risk levels. In addition to assessed risks, selection factors might include the organization's mission, environment, culture, and budget.
Monitor and assess the effectiveness of controls using pre-defined metrics	Effective testing and ongoing monitoring and evaluation can provide a level of confidence that security controls adequately mitigate the risks.

Cyber Security Policy (1)

Activity / Security Control	Rationale
Assign responsibility or developing, implementing, and enforcing cyber security policy to a senior manager. Ensure that the senior manager has the requisite authority across departments to enforce the policy.	The development and implementation of effective security policies, plans, and procedures require the collaborative input and efforts of stakeholders in many departments of the organization. Assigning a senior manager to organize and drive the efforts, with the authority to make and enforce decisions at each stage, raises the chances of success.
Define security-related roles and responsibilities.	Employees at every organizational level have some kind of responsibility in developing or applying security policies and procedures. Defined roles and responsibilities will clarify decision-making authority and responsibility at each level, along with expected behavior in policy implementation. Creating a multidisciplinary oversight committee ensure all stakeholders are represented.
Identify security aspects to be governed by defined policies.	An effective security program requires policies and procedures that address a wide range of management, personnel, operational, and technical issues.

Cyber Security Policy (2)

Activity / Security Control	Rationale
Document a brief, clear, high-level policy statement for each issue identified.	The high-level policy statements express three things: • The organization management's commitment to the cyber security program • The high-level direction and requirements for plans and procedures addressing each area • A framework to organize lower-level documents
Reference lower-level policy documents.	Lower-level policies, plans, and procedures give the details needed to put policy into practice.
Define the implementation plan and enforcement mechanisms.	A careful roll-out of the program, well-documented policies that are accessible to personnel they affect, and clearly communicated consequences of violating policies will help ensure compliance.
Define a policy management plan.	This will help maximize compliance by providing mechanisms to— • Request, approve, document, and monitor policy exceptions • Request, approve, implement, and communicate changes to policies, plans, and procedures.

Personnel and Training

Activity / Security Control	Rationale
Adequately vet candidates for hire.	Provide a level of confidence that new hires are trustworthy.
Establish a security-awareness program.	Ensure that all personnel have an understanding of sensitive information and common security risks, and basic steps to prevent security breaches. Further, ensure that personnel develop habits that would make them less susceptible to social engineering attacks.
Train employees who have access to protected assets.	Ensure that employees who have electronic or physical access to critical assets know how to handle the assets securely and how to report and respond to cyber security incidents.
Enforce "least privilege" access to cyber assets and periodically review access privileges.	Ensure that employees have only the privileges they need to perform their jobs.

Operational Risks

Activity / Security Control	Rationale
Perform periodic risk assessment and mitigation, including threat analysis and vulnerability assessments.	Maintain a fresh picture of the effectiveness of the organization's security control versus threats facing the organization.
Control, monitor, and log all access to protected assets.	Prevent unauthorized access to assets; Detect unauthorized access to assets; Enforce accountability.
Redeploy or dispose of protected assets securely.	Ensure that the redeployment or disposal of cyber assets does not inadvertently expose sensitive information to unauthorized entities.
Define and enforce secure change control and configuration-management processes.	Ensure that system changes do not "break" security controls established to protect cyber assets.
Create and document incident-handling policies, plans, and procedures.	Ensure that the organization is prepared to act quickly and correctly to avert or contain damage after a cyber security incident.
Create and document contingency plans and procedures.	Ensure that the organization is prepared to act quickly and correctly to recover critical assets and continue operations after a major disruption.
Train employees in incident handling and contingency plans.	Ensure that personnel responsible for responding to cyber incidents or major disruptions have a firm grasp of response plans and can execute them under stress.

Insecure SDLC Risks

Activity / Security Control	Rationale
Document Misuse / Abuse Cases	Think of ways in which system functionality can be abused so that protections can be built in to prevent that abuse.
Document Security Requirements	Explicitly call out security requirements of the system so that software can be designed, implemented, and tested to ensure that these requirements have been met.
Build a Threat Model	Enumerate the ways in which an adversary may try to compromise the system so that the system can be designed from the get go to resist these attacks.
Perform Architecture Risk Analysis	Compare the system's architecture against a threat model to ensure that sufficient security controls are in place to prevent successful attacks.
Define Secure Implementation Guidelines	Ensure that developers use defensive programming techniques when implementing the system in order to avoid introducing security weaknesses.

Insecure SDLC Risks

Activity / Security Control	Rationale
Perform Secure Code Reviews	Ensure that software complies with security implementation guidelines, that security controls are properly implemented, and that the implementation itself does not introduce any new security risks.
Perform Risk Based Security Testing	Run through top risks identified during threat modeling and architecture risk analysis process to ensure that the system has been designed and implemented in a way that mitigates these risks.
Have Penetration Testing Conducted	Gain assurance from a qualified third party that the software built by your organization is secure.
Build a Secure Deployment and Operations Guide	Provide the teams deploying and operating the software in production with whatever knowledge they need to have to ensure that software security requirements are met.

Physical Security Risks

Activity / Security Control	Rationale
Document, implement, and maintain a physical security plan.	Ensures that physical security is considered in a structured manner that can be tracked.
The organization must document and implement the technical and procedural controls for monitoring physical access at all access points at all times.	Ability to detect unauthorized access attempts. Take appropriate action if unauthorized access occurred.
All physical access attempts (successful or unsuccessful) should be logged to a secure central logging server.	Ability to detect unauthorized access attempts. Take appropriate action if unauthorized access occurred.
Physical access logs should be retained for at least 90 days.	Ability to perform historical analysis of physical access.
Each physical security system must be tested at least once every three years to ensure it operates correctly.	Ensure that proper physical security posture is maintained.
Testing and maintenance records must be maintained at least until the next testing cycle.	Ability to understand what was tested and improve testing procedures.
Outage records must be retained for at least one calendar year.	Ability to investigate causes of outages and tie them to unauthorized physical access.

Third-Part Relationship Risks (1)

Activity / Security Control	Rationale
Perform due diligence on each vendor and partner organization to understand their business, financial, and security track record	Verify business, financial, and security reputation of your vendor / partner organization.
Ask the right questions during the RFP process to understand the security posture and practices at the partner organization, and also understand whether their offerings meet the security requirements as defined by the cooperatives. Compare the security policies and procedures of a third party against your organization's own security policy to ensure compliance.	Ensure the security practices at the vendor / partner organization comply with your own organization's security policy. Ensure that the purchased product / service meets your organization's security requirements.
Review the hiring and personnel background checks practices of your vendors and partners to ensure that they comply with your organization's policies	Make sure that your vendor / partner organization's background checks during hiring process are consistent with your own. If people who work at your vendor / partner are not trustworthy, nor is anything they produce.
Conduct periodic audits and monitoring of the third-party organization to ensure adherence to their security policies and procedures	Make sure that your vendor / partner complies with their own security policies and procedures.

Third-Part Relationship Risks (2)

Activity / Security Control	Rationale
For software purchases, request a trusted independent third-party review and report outlining the discovered security weaknesses in the product	Increased guarantee that the product supplied by your vendor / partner is secure.
Ensure that service level agreement (SLAs) and other contractual tools are properly leveraged to ensure that vendors and partners live up to their obligations. For instance, if a breach occurs at a partner organization, there needs to be a provision to have your organization notified of the full extent of the breach as soon as the information is available	Contractual obligation that helps your organization transfer some of the security risks.
Request evidence from software vendors that their software development lifecycle makes use of building security in activities	Ensure that the product supplied to your organization by your vendor / partner has been designed and built with security in mind
Ask your organizations' vendors and partners about the process that they use to ensure security of the components and services that they receive from their own suppliers to ascertain appropriate due diligence.	Ensure that none of the third party components that your vendor / partner used in their product introduce security weaknesses.

Network Risks (1)

Activity / Security Control	Rationale
Restrict user-assigned devices to specific network segments	Least privilege through network segmentation
Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic from network segment to another of a different security level should default to a 'deny all' stance.	Security by default
Requests for allowing additional services through a firewall or other boundary protection mechanisms should be approved by the Information Security Manager.	Centrally managed access driven by business need
The flow of electronic communications should be controlled. Client systems should communicate with internal servers; these internal servers should not communicate directly with external systems, but should use an intermediate system in your organization's DMZ. The flow of traffic should be enforced through boundary protection mechanisms.	Confine sensitive electronic communication to established trust zones.
Protect data in transit.	Preserve confidentiality and integrity of data in transit.
Protect DNS traffic.	Ensure that data is routed to the right parties.
Use secure routing protocols or static routes.	Avoid information disclosure of internal routing
Deny use of source routing.	Prevent denial of service attacks

Network Risks (2)

Activity / Security Control	Rationale
Use technologies like firewalls and virtual LANs (VLANs) to properly segment your organization's network to increase compartmentalization (e.g., machines with access to business services like e-mail should not be on the same network segment as your SCADA machines). Routinely review and test your firewall rules to confirm expected behavior.	Achieve network segmentation to achieve compartmentalization
Separate development, test, and production environments.	Avoid production data leaks into test environments. Have controls in place around access to and changes in the production environment.
Ensure channel security of critical communication links with technologies like Transport Layer Security (TLS). Where possible, implement Public Key Infrastructure (PKI) to support two-way mutual certificate-based authentication between nodes on your network.	Secure data in transit
Ensure that proper certificate and key management practices are in place. Remember that cryptography does not help if the encryption key is easy to compromise. Ensure that keys are changed periodically and that they can be changed right away in the event of compromise.	Ensure that cryptographic protection is not undermined through improper certificate or key management

Network Risks (3)

Activity / Security Control	Rationale
Ensure confidentiality of data traversing your networks. If channel level encryption is not possible, apply data level encryption to protect the data traversing your network links.	Secure data in transit
Ensure integrity of data traversing your networks through use of digital signatures and signed hashes. If TLS not used, ensure that other protections for man in the middle attacks exist. Use time stamps to protect against replay attacks.	Preserve data integrity
Ensure availability of data traversing your networks. If a proper acknowledgement (ACK) is not received from the destination node, ensure that provisions are in place to resend the packet. If that still does not work, reroute the packet via a different network link. Implement proper physical security controls to make your network links harder to compromise.	Detect failures and promote fault tolerance
Ensure that only standard, approved, and properly reviewed communication protocols are used on your network.	Use proven protocols that have been examined for security weaknesses
Use intrusion detection systems (IDS) to detect anomalous behavior on your network. If anomalous behavior is encountered, have a way to isolate the potentially compromised nodes from the rest of the network.	Detect intrusions

Network Risks (4)

Activity / Security Control	Rationale
Ensure that a sufficient number of data points exist from devices on your network before the smart grid takes any actions based on that data. Never take actions based on the data coming from network nodes that may have been compromised.	Avoid taking actions based on incorrect data.
Ensure that all settings used on your network hardware have been set to their secure settings and that you fully understand the settings provided by each piece of hardware. Do not assume that default settings are secure.	Secure configuration
Disable all unneeded network services.	Reduce attack surface
Routinely review your network logs for anomalous / malicious behavior via automated and manual techniques.	Intrusion detection
Ensure that sufficient redundancy exists in your network links so that rerouting traffic is possible if some links are compromised.	Continuity of operations
Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual (i.e., non-shared) credentials.	Enforce accountability

Network Risks (5)

Activity / Security Control	Rationale
Limit remote access to your networks to an absolute minimum. When required, use technologies like Virtual Private Networks (VPN) to create a secure tunnel after properly authenticating the connecting party using their individual credentials. In addition to user name and password, also use a separate technology (an RSA ID-like device) to provide an additional factor of authentication.	Prevent unauthorized access
Implement remote attestation techniques for your field devices (e.g., smart meters) to ensure that their firmware has not been compromised	Prevent unauthorized modification of firmware on field equipment
Require a heart beat from your field equipment at an interval known to the piece of equipment and to the server on your internal network. If a heart beat is missed or comes at the wrong time, consider treating that piece of equipment as compromised / out of order and take appropriate action.	Detect tampering with field equipment
Ensure that the source of network time is accurate and that accurate time is reflected on all network nodes for all actions taken and events logged.	Maintain accurate network time
Document the network access level that is needed for each individual or role at your organization and grant only the required level of access to these individuals or roles. All exceptions should be noted.	Maintain control and least privilege of access to network resources
All equipment connected to your network should be uniquely identified and approved for use on your organization's network.	Control hardware that gets connected to your organization's network

Platform Risks (1)

Activity / Security Control	Rationale
Ensure latest security patches are applied to all software running on your network hosts	Patch known weaknesses so that they cannot be exploited
Ensure the latest antivirus / antimalware software runs regularly	Detect known viruses and/or malware
Ensure that all unneeded services and interfaces (e.g., USB interface) are turned off on these hosts.	Minimize attack surface
Ensure that the hosts run only services and applications that are absolutely necessary	Minimize attack surface
Ensure that system logs are checked regularly and any abnormalities are investigated	Detect intrusions / attack attempts (both external and internal)
Run software to monitor for file system changes.	Detect system malware infections and unauthorized changes
Ensure that all access attempts and any elevation of privilege situations are properly logged and reviewed.	Detect intrusions / attack attempts (both external and internal)
Ensure that passwords are of sufficient complexity and changed periodically.	Prevent unauthorized access
Ensure that all security settings on your hosts are configured with security in mind.	Prevent unauthorized access

Platform Risks (2)

Activity / Security Control	Rationale
Ensure that authentication is required prior to gaining access to any services / applications running on your network hosts and that it cannot be bypassed.	Prevent unauthorized access
Make use of a centralized directory like LDAP to manage user credentials and access permissions. Ensure that users have only the minimum privileges needed to do their job functions. If an elevation of privilege is needed, grant it for the minimum amount of time needed and then return the privileges to normal.	Enforce the principle of least privilege; Prevent unauthorized access; Make it easy to change passwords; Make it easy to revoke access; Make it easy to enforce password complexity;
Ensure that all software updates are properly signed and coming from a trusted source.	Malware protection
Prevent the ability to change field device settings without proper authentication. Changes to field device settings should be reported and logged in a central location. These logs should be reviewed frequently.	Maintain confidence in data coming from field devices by ensuring that they have not been tampered with
If possible, verify integrity of firmware running on field equipment via remote attestation techniques. Consult with the equipment vendor for assistance. If remote attestation fails, the affected field device should be considered compromised, and should be isolated.	Maintain confidence in data coming from field devices by ensuring that they have not been tampered with

Application Layer Risks

Activity / Security Control	Rationale
Implement security activities and gates into your organization's software development lifecycle (SDLC) (please refer to checklist under "Insecure SDLC Risks" section for additional detail)	Your organization develops software that does not have security weaknesses
Request independent party software security assessments of the applications being purchased to gauge the software's security posture.	Gain confidence that third party software your organization purchases does not have security weaknesses

Advanced Metering Infrastructure (1)

Activity / Security Control	Rationale
Ask software and hardware (with embedded software) vendors for evidence (e.g., third-party assessment) that their software is free of software weaknesses	Ensure that smart meters and their data are not compromised
Perform remote attestation of smart meters to ensure that their firmware has not been modified	Ensure that smart meters and their data are not compromised
Make use of the communication protocol security extensions (e.g., MultiSpeak® security extensions) to ascertain the data integrity and origin integrity of smart meter data	Ensure that smart meters and their data are not compromised
Establish and maintain secure configuration management processes (e.g., when servicing field devices or updating their firmware)	Ensure that smart meters and their data are not compromised
Ensure that all software (developed internally or procured from a third party) is developed using security aware SDLC.	Ensure that smart meters and their data are not compromised
Apply a qualified third party security penetration testing to test all hardware and software components prior to live deployment	Ensure that smart meters and their data are not compromised

Advanced Metering Infrastructure (2)

Activity / Security Control	Rationale
Decouple identifying end user information (e.g., household address, GPS coordinates, etc.) from the smart meter. Use a unique identifier instead.	Preserve user privacy
Implement physical security controls and detection mechanisms when tampering occurs	Ensure that smart meters and their data are not compromised
Ensure that a reliable source of network time is maintained	Ensure that timely smart grid decisions are taken based on fresh field data
Disable remote disconnect feature that allows to shut down electricity remotely using a smart meter	Prevent unauthorized disruption / shutdown of segments of the electrical grid

Meter Data Management

Activity / Security Control	Rationale
Data arriving to be stored in the MDM does not come from a compromised meter	Only data from uncompromised meters is stored in the MDM
Data arriving to be stored in the MDM is syntactically and semantically valid	Prevent storing bad data in MDM and prevent potentially harmful / malicious data from compromising the system
The system parsing the data arriving in the MDM should make use of all the appropriate data validation and exception handling techniques	Prevent storing bad data in MDM and prevent potentially harmful / malicious data from compromising the system
The MDM system has been designed and implemented using security aware SDLC	Prevent storing bad data in MDM and prevent potentially harmful / malicious data from compromising the system
The MDM system had passed a security penetration test by a qualified third party	Prevent storing bad data in MDM and prevent potentially harmful / malicious data from compromising the system
Cleanse data stored in the MDM from all private information.	Promote user privacy
Gracefully handle denial of service attempts (from compromised meters)	Protect MDM system from attacks originating from smart meters

Communication Systems (1)

Activity / Security Control	Rationale
Ensure data integrity	Secure communications
Ensure origin integrity	Secure communications
Use proven communications protocols with build in security capabilities	Secure communications
Ensure confidentiality of data where appropriate	Secure communications
Ensure proper network segmentation	Compartmentalization, least privilege, isolation, fault tolerance
Have a third party perform network security penetration testing	Higher assurance that communications are secure
Implement sufficient redundancy	Fault tolerance
Protect from man in the middle attacks	Secure communications
Protect from replay attacks	Secure communications
Use proven encryption techniques	Secure communications
Use robust key management techniques	Secure communications

Communication Systems

Activity / Security Control	Rationale
Ensure data integrity	Secure communications
Ensure origin integrity	Secure communications
Use proven communications protocols with build in security capabilities	Secure communications
Ensure confidentiality of data where appropriate	Secure communications
Ensure proper network segmentation	Compartmentalization, least privilege, isolation, fault tolerance

SCADA (1)

Activity / Security Control	Rationale
Appoint a senior security manager with a clear mandate	Make security somebody's responsibility
Conduct personnel security awareness training	Help improve the people aspect of security
Apply basic network and system IT security practices (e.g., regular security patches, run antivirus, etc.)	Make your SCADA environment more difficult to compromise
Ensure that software running in the SCADA environment (e.g., either internal or external) has been built with security in mind and reviewed for security by a qualified third party	Protect from the perils of insecure software
Enforce the principle of least privilege granting user access to SCADA resources	Least privilege of access
Ensure proper physical security controls	Supplement IT security controls with physical controls
Perform monitoring, logging, and ensure that people can be held accountable for their actions	Intrusion detection, forensic analysis, holding people accountable.
Avoid making critical control decisions without human confirmation	Put the human operator in control

SCADA (2)

Activity / Security Control	Rationale
Avoid making critical control decisions based on too few data points	Avoid taking erroneous actions at the SCADA level
Avoid taking critical control decisions based on data points from compromised field devices or based on data that has been tampered with	Avoid taking erroneous actions at the SCADA level
Ensure proper network segmentation in the SCADA environment	Segregate critical control systems from the rest of your organization's corporate environment to promote compartmentalization
Ensure sufficient fault tolerance and redundancy in the SCADA environment	Plan for failure and continuation of operations
Develop and test business continuity and disaster recovery plans	Plan for failure and continuation of operations
Use individual (rather than shared) user login accounts with strong passwords	Prevent unauthorized access and promote accountability.
Ensure that all hardware authentication settings have been changed from their default values	Prevent unauthorized access

In Home Displays & Web Portals

Activity / Security Control	Rationale
Ensure that the software running on the in home displays are free of software weaknesses, especially if they are remotely exploitable.	Ensure that attackers cannot remotely control IHDs of users
Ensure the integrity of data shown on the user's in home display	Integrity of data sent to the user
Ensure the anonymity and privacy of data (where appropriate) pertaining to electricity usage patterns such that it cannot be tied back to the consumer	Privacy of user's electrical usage data
Perform remote attestation of IHDs to alert the control center when unauthorized firmware updates occur	Knowing when IHDs have been tampered with and should not longer be trusted
Request third party security penetration testing of IHDs	Assurance that deployed system has an adequate security posture

Demand Response Over AMI

Activity / Security Control	Rationale
Same activities and security controls described in the "AMI" section above	
Authenticate and validate all control signals coming from the control center to the smart meters	Prevent unauthorized control of electric devices in the consumer's home
Provide consumers a feature to turn off remote control of in house electric devices via smart meters in the event that meters become compromised. Financial penalties should apply however if this action is taken frivolously where no evidence of meter compromise exists.	Consumers should have a default overwrite ability if their smart meters become compromised. However, financial penalties should apply if consumers make use of default overwrite capability frivolously.

Interactive Thermal Storage

Activity / Security Control	Rationale
Ensure that the software running on the device controlling the electrical water heaters is free of software weaknesses, especially if they are remotely exploitable.	Ensure that attackers cannot remotely control electrical water heaters of users
Request third party security assessment of all software used to control the electrical water heater	Ensure that attackers cannot remotely control electrical water heaters of users
Conduct a security penetration test	Ensure that attackers cannot remotely control electrical water heaters of users
Build in mechanism to authenticate and validate control signals for the electrical water heater	Ensure that attackers cannot remotely control electrical water heaters of users
Built in safe guards into the operation of the electrical water heater (e.g., never go above a certain temperature, etc.). This should already come standard on most if not all water heaters.	Ensure human safety
Provide a manual override mechanism where users can prevent their electrical heater from being controlled remotely	Ensure human safety

Advanced Volt/VAR Control

Activity / Security Control	Rationale
Ensure that software controlling distribution feeders is free of security weaknesses	Prevent unauthorized control of distribution feeders
Implement physical security controls and detection mechanisms when tampering occurs	Prevent unauthorized control of distribution feeders
Perform sufficient authentication and validation of all control data bound for distribution feeders	Prevent unauthorized control of distribution feeders
Ensure that a human(s) has to review and authorize any changes to electrical distribution feeders	Prevent unauthorized control of distribution feeders
Ensure that there are built in safeguards in hardware	Ensure safe behavior when failures occur

Conservation Voltage Reduction

Activity / Security Control	Rationale
Ensure that software controlling voltage regulators and monitors is free of security weaknesses	Prevent unauthorized voltage reduction behavior
Implement physical security controls and detection mechanisms when tampering occurs	Prevent unauthorized voltage reduction behavior
Perform sufficient authentication and validation of all control data bound for voltage regulators and coming from voltage monitors	Prevent unauthorized voltage reduction behavior
Ensure that a human(s) has to review and authorize any changes to voltage	Prevent unauthorized voltage reduction behavior
Ensure that there are built in safeguards in hardware	Ensure safe behavior when failures occur