Vulnerability Assessment for Critical Infrastructure Control Systems

Assessing the security of critical infrastructure control systems without understanding those systems can cause dangerous real-world consequences. This guide for security assessors is founded on work that supports a current security standard and relates it to traditional IT security assessment.

Assessing critical infrastructure control systems security isn’t like assessing business and government information systems security. Control system equipment can be more fragile than standard IT systems. Moreover, using standard enumeration and scanning techniques on control systems can create failures with serious real-world consequences—for example, we know of one incident in which IT assessors left a natural gas pipeline’s control center without a view of the pipeline’s state for an entire shift.

Control systems manage the physical processes that involve hazardous environments, substances, and other processes that can lead to loss of life. Given these stakes, providing guidance for IT security assessors to work in the control system world is vital. Accordingly, industry groups, government agencies, the research community, and control system owners and operators are working together to increase control system security.

As part of this effort, Sandia National Laboratories has worked with electric industry partners to develop the tools to perform a control system security assessment specific to the electric sector and current standards. Although our assessment process is customized to the electric industry, we used Sandia’s general assessment methods and tools to make it applicable to other types of control systems. Our steps—including planning, conducting, reporting, and concluding—should be familiar to anyone who’s performed an information system security assessment. Assessors can use the four-step process, their experience, and this guide to assess any critical infrastructure control system.

Standards for Control Systems Security

Control system security standards must differ from existing general IT security standards because their business and mission goals differ. The major difference is in how each prioritizes the canonical security goals of confidentiality, integrity, and availability. In business and commerce systems, confidentiality is the highest priority, followed closely by integrity; availability is rarely deemed equally important. In contrast, in control systems, availability is most important, far outstripping confidentiality and even integrity. A business Web site or email system can easily afford a few minutes of down time, but if a control system operator loses the view of the physical process, the consequences can be catastrophic.

The Critical Infrastructure Protection Standards

The North American Electric Reliability Corporation’s Critical Infrastructure Protection standards (www.nerc.com/~filex/standards/Reliability_Standards.html) establish the minimum requirements to ensure electronic information exchange security to support the bulk power grid’s reliability. NERC adopted the CIP-002 through CIP-009 standards in May 2006 after several years of consensus building within the electric industry. In July 2006, the Federal Electric Reliability Commission issued an order certifying NERC as the Electric Reliability Organization under the Federal Power Act. This in turn made the NERC CIP standards into regulations.

The NERC CIP standards address security as a...
process to solve a system problem. CIP-002 starts the security process by identifying the electric grid’s critical assets. It further requires that the control system components that control critical assets be considered critical cyber assets. Following from this,

- CIP-003 sets the security management standard,
- CIP-004 discusses personnel security,
- CIP-005 gives utilities a standard for electronic security perimeters to protect critical cyber assets,
- CIP-006 covers physical security,
- CIP-007 standardizes the security management of critical cyber assets,
- CIP-008 provides incident reporting and response requirements, and
- CIP-009 offers standards for recovery.

Both CIP-005 and CIP-007 require annual cyber vulnerability assessments (CVAs). Although the utilities can choose the assessments’ form, they must meet certain minimum requirements.

**Sandia’s Role**

In 1996, Sandia National Laboratories began working with the President’s Commission on Critical Infrastructure Protection. This work led to the 1998 Presidential Decision Directive 63, which called for critical infrastructure protection by reducing vulnerabilities through a public–private partnership. Since that time, the US government has given increasing attention to computer and information systems that control critical infrastructures. Homeland Security Presidential Directive 7, issued in 2003, for example, focuses on the need to protect information systems supporting telecommunications, chemical, oil, gas, and electric infrastructures.

Since 1996, Sandia has helped secure the nation’s critical infrastructures by assessing flood control, irrigation, and hydroelectric dams; water systems; oil refineries; oil and gas pipelines; and electric transmission, generation, and distribution systems. Furthermore, private owners of critical infrastructure have all worked to improve their information system security, focusing on systems that control the infrastructures’ physical processes.

**Process Limits and Requirements**

Our process doesn’t answer questions about how to prioritize vulnerabilities for mitigation, the consequences of vulnerability exploitation, or the likelihood of a particular adversary attacking the system. Other processes exist that take assessments in those directions, including Sandia’s Risk Assessment Methodology (www.sandia.gov/ram) family and Information Design Assurance Red Team methodology (www.sandia.gov/idart). In keeping with the requirements outlined in CIP 005 and 007, our assessment discovers security possibilities but makes no attempt to determine the probability of an attack or an undesired consequence. Such questions require considerably more analysis.

To understand why we developed the assessment process as we did, it’s important to examine the CIP requirements that drive it. Among the NERC CIP-005 Electronic Security Perimeter requirements is R4, which states that the CVA must examine the ESP’s electronic access points at least annually. At a minimum, that assessment must include

- R4.1. A document identifying the vulnerability assessment process;
- R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
- R4.3. The discovery of all access points to the Electronic Security Perimeter;
- R4.4. A review of controls for default accounts, passwords, and network management community strings; and
- R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007 includes R8, which states that the CVA must assess all the ESP’s cyber assets at least annually. At a minimum, that assessment must include

- R8.1. A document identifying the vulnerability assessment process;
- R8.2. A review to verify that only ports and services required for operation of the cyber assets within the Electronic Security Perimeter are enabled;
- R8.3. A review of controls for default accounts; and
- R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

As the CIP-005 requirements clearly indicate, the interaction between the ESP and the physical security perimeter (PSP) specified in CIP-006 is key. As CIP-006 states,


Such requirements determine the CIP CVA’s nature as well as its scope. Much of the work to meet both requirements is the same, so the assessment should be
a single activity with the dual goal of satisfying the two primary requirements.

The requirements have commonalities—for example, the TCP/IP ports, access accounts, and services running on all cyber assets in or protecting the ESP should be documented in both types of CIP CVA. The need to determine account security also applies to both requirements. The differences arise in determining access from outside the ESP. CIP-005 requires the discovery of all electronic access points. Thus, we can see that the CIP CVA process must answer the requirements of CIP-005 and CIP-007 while also meeting CIP-006’s requirements. To save resources, the assessment team can take advantage of overlaps when collecting data, but the team must analyze that data separately for each CIP standard requirement.

The requirements have commonalities—for example, the TCP/IP ports, access accounts, and services running on all cyber assets in or protecting the ESP should be documented in both types of CIP CVA. The need to determine account security also applies to both requirements. The differences arise in determining access from outside the ESP. CIP-005 requires the discovery of all electronic access points. Thus, we can see that the CIP CVA process must answer the requirements of CIP-005 and CIP-007 while also meeting CIP-006’s requirements. To save resources, the assessment team can take advantage of overlaps when collecting data, but the team must analyze that data separately for each CIP standard requirement.

The Cyber Vulnerability Assessment Process

Once the responsible entity commits to meeting the requirements discussed earlier, the CIP CVA process begins. Typically, the responsible entities—which might be public or private utilities providing generation, transmission, or distribution of electricity and their supervising authorities—hire an outside assessment team. The process results produce a detailed understanding of the ESP and system services, so the responsible entity can use a first assessment’s results to satisfy other documentation requirements. For example, the team might use an initial CIP CVA to fulfill both that assessment’s requirement and the initial requirement for ESP documentation (CIP-005, R1.6).

The assessment team must complete a CIP CVA according to four steps: planning for the assessment, conducting the assessment, reporting the results, and planning mitigation once the report is accepted.

Assessment Planning

In planning the CVA, team members must collaborate closely with the responsible entity’s operations and engineering personnel. System and network administration personnel support assessments by providing data and access. This can put stress on key personnel—especially in conjunction with additional audits, assessments, system changes, or other activities. The team and utility should therefore schedule the assessment when operational stresses are unlikely to complicate the situation. For example, some regions have bad weather that causes outages during certain seasons, so adding the stress of an assessment to that of responding to outages will cause problems for the operations and engineering personnel who must work with the assessment.

Scope, requirements, and resources. In planning the assessment, the team leader must first determine the CVA’s scope on the basis of five key questions:

- How long will it take?
- How many assessors will we need?
- How will data be collected?
- Who will collect the data?
- How many systems will we assess at how many locations?

To identify systems and facilities to be assessed, the team leader must work with the assessment customer. The customer might, for example, want the team to perform a complete CIP CVA of all critical cyber assets, including control centers, generation plants, substations, and remote access points such as power broker offices. Alternately, the customer might distribute a complete assessment among multiple assessment teams.

The number and type of critical cyber assets and the applications that they execute help determine the CVA project’s scope. The ESP’s size also affects the scope; larger enclaves imply more complex internal network infrastructure requiring more assessment. The number of ESPs and communication paths between them are also important considerations.

Next, the team leader must determine performance requirements. Here again, the number of ESPs and their communication paths are key, as are the number and location of critical cyber assets. In the third step, the leader estimates the resources required, based on experience, past assessments, and the project’s scope. Sandia has prepared some planning tools—a spreadsheet and Microsoft Project plan—that incorporate our experience with past assessments. Travel is a given in performing CIP CVAs. If the assessing and assessed organizations are in the same location, travel costs will be limited to trips to outlying locations, such as alternate control centers, generation plants, and substations. More likely, however, the assessment organization is based elsewhere and thus travel, lodging, and food expenses contribute significantly to the assessment’s total cost.

Rules of engagement. Some cybersecurity assessments are merely paper exercises. The CIP CVA, however, requires active engagement. The assessors must access—or watch others access—critical cyber assets within the responsible entity’s control systems. The assessment team leader must therefore work with his or her counterpart in the responsible organization to develop rules for activities that both protect the organization’s operation and limit the assessment team’s liability. These rules of engagement should indicate which activities will take place in which systems and who can perform them.

The engagement rules also cover decisions on whether activities take place within the primary active control system, a secondary control system, or an offline test system. The safest solution is to avoid any activities in the primary active control system, but if all parties agree,
passive activities—such as network sniffing—might be allowed. Credible substitutes for the active control system can include a backup or secondary control system, a testing network, or stand-alone systems. The assessors must compare all substitutes with the active systems to ensure that they’re operationally identical.

The assessment team and the responsible entity must together agree on who will have “hands on the keyboard” during active control systems access. It’s safest to have the organization’s own personnel perform all such actions with directions from the assessment team.

**Team identification.** Unless the team leader needs specialized expertise during planning, he or she selects team members in the final planning stage. Still, the assessment team leader must understand all team roles and responsibilities before beginning the planning process.

Ideally, the team leader can draw from a diverse set of people and skills to create a team that best fits the particular assessment’s requirements. For a CIP CVA, a team needs IT assessors, control systems engineers, and physical security assessors. Furthermore, the CVA’s scope, performance objectives, resource requirements, travel requirements, project plan, and rules of engagement should all inform the team selection process. Team diversity is also important—on a uniform team, members will tend to identify the same vulnerabilities. A diverse team typically discovers more vulnerabilities, even if individual members have less expertise.

The CVA team consists of several roles, the first of which is **team leader.** The team leader

- performs or supervises all assessment planning,
- leads the team during the assessment,
- manages any necessary plan changes during the assessment,
- ensures that the results are reported, and
- ensures that the responsible entity gets sufficient support during mitigation planning.

A team leader needs both managerial and technical skills. In some cases, an assessment organization might need to split the team leader role into two parts: project management and technical management.

The second role is that of **team member.** A team might consist of one or more members, depending on the target system’s size and complexity. Team members

- perform the technical assessment tasks,
- report their results, and
- support mitigation planning, if necessary.

The third role is that of **recorder.** Again, a project might have one or more recorders depending on its scope. Although recorders can serve in other roles on the assessment team, during the actual engagement, they should conduct only the following duties:

- observe and record all team members’ actions during the assessment, and
- collect and archive all team member data at the end of each day of the assessment.

Finally, a team might have one or more **report writers** depending on the project’s scope. The report writer can also play other roles, including team leader or member. The report writer’s specific duties are to collect and edit team contributions and produce the final assessment report.

**Activity scheduling and resource assessment.** Assessment activities involve two times: actual hands-on person-hours, and elapsed time for the activity. In certain cases, assessment activities involve simply setting up and executing computer programs that can take many hours to complete. In those cases, person-hour time is short, but elapsed time is long.

Also, assessment activities require different skill sets to complete. Some activities require people with considerable security assessment skills. Others must be performed by the responsible entity’s system and network administrators. Still other activities can be performed by any team member, including computer science or computer engineering graduate students without assessment experience or knowledge of the utility networks and computers. To plan properly, the team leader must understand the technical skills that their personnel resources possess.

As Table 1 shows, to successfully complete certain tasks, a CVA might require that the responsible entity provide resources with advanced access levels. In that case, the organization might grant access credentials to the assessment team; again, however, we recommend that it instead reserve access for its own personnel.

**Conducting the Assessment**

To conduct the assessment, the team “simply” carries out the assessment plan. As in warfare, however, no plan survives contact with the enemy. The CVA plan will inevitably change once the actual assessment begins and unexpected events occur, such as last-minute changes in personnel, personnel availability, and location access times. Such unexpected events are beyond the assessment team’s control, arising from communication failures and changes in direction within the responsible entity’s leadership team.

In such cases, the team leader must simply adapt the plan, reschedule tasks, and reallocate resources to fit reality. The team leader must also try to maintain task integrity within the plan, or conflicts can arise with the responsible entity’s operations. It’s better to
reschedule tasks than to subdivide them and possibly extend or fragment the active engagement period.

Assessment activities entail specific issues that a successful team leader will anticipate and adequately address, including ordering project tasks and managing the discovery process.

**Ordering project tasks.** Although project tasks are distinct, the team leader must ensure that they’re conducted not in the “project order” but in a logical order that minimizes operational disruption. Each critical asset’s services check and account check should occur simultaneously to minimize access time to the asset. Furthermore, although the external services check supplements the internal check, they don’t have to take place at the same time. Instead, the team can do internal and external activities separately, assuming they regularly check the platform to ensure it hasn’t changed.

**Managing discovery.** CIP-005 requires discovery of all electronic access points, such as LAN devices (routers, switches, and firewalls), serial devices (telephone modems and dedicated phone lines), or wireless devices (802.11 wireless access points, 802.15 Bluetooth or derivative, GPRS, or other radio). In traditional IT assessments, penetration testing using tools—such as port scanning or external access control analysis—can initially assess the virtual location of ESP ingress. However, penetration testing tools shouldn’t be used within the ESP’s boundaries.

Analyzing external access controls can provide the same information as a penetration testing tool. Fortunately, CIP-005’s R.3.2, and R.5.3 require responsible entities to retain electronic access logs for 90 days. The team can use these logs in conjunction with analysis of firewall rules and router access control lists to obtain the same information as they’d get with penetration testing. Regardless of the discovery method, the team leader must have a grounded understanding of the target systems. An unexpected penetration test result indicates that the leader wasn’t fully prepared or lacked accurate pre-engagement information about the test’s scope.

The assessment team can perform passive discovery of ESP access using tools such as Sandia’s Advanced Network Toolkit for Assessments and Remote Mapping. Antfarm accepts data sets from multiple sources containing information about network relationships. Like many other tools, it uses standard sniffer files, but it can also use network device configurations and even logs. As Figure 1 shows, Antfarm creates a database of network relationships for analysis and visualization.

For dial-up access discovery, the team should obtain an inventory of all phone numbers the utility controls. As with penetration testing, passively reviewing telephone line locations is sometimes sufficient to assert that there are no telephone modems within the ESP. However, the team can also verify this information using a “war dialing” program to find any modems connected to utility-owned telephone lines.

The team can accomplish wireless discovery by continuously monitoring the target area using commercial tools that let them map and locate rogue 802.11 access points. These are not inherently vulnerable as 802.1x authentication on Ethernet switches can protect the organization’s network from both wired and wireless rogue devices. The team might need to look

---

**Table 1. The responsible entity’s required resources.**

<table>
<thead>
<tr>
<th>REQUIREMENTS*</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC Local Admin</td>
<td>Local administrator on a particular host or hosts within the control center</td>
</tr>
<tr>
<td>CC Test Network</td>
<td>Test network separate from the operational control center network with systems that duplicate operational systems</td>
</tr>
<tr>
<td>CC Network Admin</td>
<td>Network administrator on the control center network (such as a domain administrator in a Microsoft network)</td>
</tr>
<tr>
<td>CC Network Eqpmnt Admin</td>
<td>Administrator for network equipment, such as routers, firewalls, and switches</td>
</tr>
<tr>
<td>Gen Local Admin</td>
<td>Local administrator on a particular host or hosts at a target generation plant</td>
</tr>
<tr>
<td>Gen Network Admin</td>
<td>Network administrator on the generation plant network</td>
</tr>
<tr>
<td>Gen Test Network</td>
<td>Test network separate from the generation plant’s distributed control system using systems that duplicate DCS operational systems</td>
</tr>
<tr>
<td>Gen Network Eqpmnt Admin</td>
<td>Administrator for network equipment, such as routers, firewalls, and switches</td>
</tr>
<tr>
<td>Substation Engineer</td>
<td>Engineer responsible for the design and maintenance of a substation and its control system equipment</td>
</tr>
<tr>
<td>Substation Local Admin</td>
<td>Local administrator on a particular host or hosts at a target substation</td>
</tr>
<tr>
<td>Substation Network Admin</td>
<td>Network administrator on the substation networks</td>
</tr>
<tr>
<td>Substation Network Eqpmnt Admin</td>
<td>Administrator for network equipment, such as routers, firewalls, and switches</td>
</tr>
</tbody>
</table>

*CC—control center; Admin—administrator; Gen—generation; Eqpmnt—equipment
inside the network to discover whether 802.1x authentication is used. If the target organization doesn’t have dedicated wireless discovery tools in place, the team should scan the ESP’s physical perimeter using a mobile device to ensure no wireless access points are unaccounted for inside the ESP.

The team should evaluate access points and internal control system network systems using representative test systems. To do this, the team must first confirm that the test systems are actually representative of the critical cyber assets by comparing services and accounts information collected from both.

**Reporting the Results**

The key goal in results reporting is to provide actionable information. The CIP standards mandate that the responsible entity present a document that contains the following:

- a description of the CVA process;
- documentation of the assessment results;
- an action plan to remediate or mitigate vulnerabilities; and
- the execution status of that action plan.

The responsible entity takes or derives all but the last item from the assessment report. The report should therefore include a full assessment process description. The team reporter can derive this from the assessment plan, but the actual description must include enough specific technical information so that the responsible entity can ask others to duplicate the results. Furthermore, the report should identify specific tools, methods, and techniques for future use, as well as offer sufficient information to assure auditors that the assessment process fulfills CIP requirements.

The assessment report should identify all vulner-
abilities found during the assessment. Although this seems obvious, the key to making vulnerability reports useful is to link them to the assessment process and to all the circumstances that enable vulnerability.

In the report’s vulnerability section, the reporter must record specific information as well as information about the tools, methods, and techniques that the team used to collect it. One unfortunate security assessment reality is that the tools we use today might not be available tomorrow. In such a case, a future assessor might not be able to use the same tool to determine whether a vulnerability still exists. However, given sufficient information on the vulnerability and the tool previously used to detect it, the assessor can find an equivalent tool.

A vulnerable service or outdated user login doesn’t constitute a vulnerability on a critical cyber asset. This is particularly true in CIP CVAs that are linked to physical security. If all control center operators use the same login, for example, this might appear to be a vulnerability, but if the control center’s physical access controls allow only those operators to enter, the PSP components provide strong authentication. In any case, the assessment report must show how a credible adversary could (or could not) exploit that service or login as a vulnerability. Given such information, the responsible entity can choose from any needed mitigation strategies and ensure mission performance.

Ultimately, there’s no point to any assessment—let alone a security assessment—if the assessed organization doesn’t use the resulting report. Assessors must provide enough information to let the responsible entity make an informed choice about mitigation strategies. Although assessors should avoid getting deeply involved in planning and executing the mitigation—to preserve perspective and objectivity—they can make general recommendations. Finally, the assessors should be available to the mitigation planning team to offer information and critical feedback.

**Planning Mitigation**

NERC CIP requirements address the final and most important step of the assessment process: mitigating the discovered vulnerabilities. To comply with the NERC CIP Vulnerability Assessment Requirements, the assessment team and responsible entity must document three things: the assessment’s results, the action plan for remediating or mitigating the identified vulnerabilities, and the action plan’s execution status.

Although the assessment team can participate in the mitigation process, they must maintain objectivity if they’re expected to assess the mitigation results for the next year’s assessment. Sandia typically addresses this by asking the assessment team to make only general recommendations for mitigation, even when reviewing the mitigation plan.

Mitigation plans must include some analysis that helps the responsible entity prioritize the vulnerabilities. No entity—utility or otherwise—can afford to fix all vulnerabilities. The vulnerabilities must therefore be ranked according to risk, which requires more information and analysis than will typically emerge from the CIP CVA process.

To address this, analysts at Sandia’s Information Design Assurance Red Team first develop attacks that use the vulnerabilities and then determine the indicators for each attack step. The analysts then match the attack indicators against models that show adversary capabilities to see which attacks they can perform. Although this process is outside the CIP CVA’s scope, it could be a valuable adjunct for planning mitigation.

Assessing the vulnerability of control systems for critical physical processes requires careful planning and execution. Although the process we propose here was developed specifically for the electrical sector, it can be generalized to control systems in other sectors including oil and gas, water and wastewater, and possibly even telecommunications.

Other control systems assessors offered feedback on our work and indicated a need for process optimization. We believe that careful scheduling and project planning will bring the elapsed time and labor hours below our initial projections. Also, our experiences with more recent assessments indicate that we need to revise our tools and methodologies to suit increasingly complex environments. The tools and methods we used to develop this guide are already obsolete in the face of larger networks and complex environments. Finally, research in the energy sector has resulted in other tools that might be useful adjuncts to this process.

Raymond C. Parks is a member of the Information Design Assurance Red Team at Sandia National Laboratories, where he’s a senior technical staff member in the Assurance Technology and Assessments Department. His research interests are in process control systems and he’s working to develop tools to make PCS assessment easier and safer. Parks has a BS in engineering from the US Air Force Academy. Contact him at rcparks@sandia.gov.

Edmond Rogers is a security analyst at a Fortune 500 electric utility and a member of the Control Systems Security Working Group of the North American Electric Reliability Corporation (NERC). His job duties include penetration testing for control networks, ensuring policy compliance, and providing risk assessment guidance to management. He’s also responsible for the cybersecurity aspects of the NERC CIP 002-009. Rogers is a Certified Information Systems Security Professional and a member of NERC’s Control Systems Security Working Group. Contact him at edmond.rogers@gmail.com.