INL/EXT-16-40341

Consequence Prioritization Process for Potential High Consequence Events (HCE)

Mission Support Center

Idaho National Laboratory

October 31, 2016

This page intentionally left blank

Contents

Tables

Figures

This page intentionally left blank

1 Introduction

This document describes the process for Consequence Prioritization, the first phase of the Consequence-Driven Cyber-Informed Engineering (CCE) framework. The primary goal of Consequence Prioritization is to identify potential disruptive events that would significantly inhibit an organization's ability to provide the critical services and functions deemed fundamental to their business mission. These disruptive events, defined as High Consequence Events (HCE), include both events that have occurred or could be realized through an attack of critical infrastructure owner assets. While other efforts have been initiated to identify and mitigate disruptive events at the national security level, such as Presidential Policy Directive 41 (PPD-41), this process is intended to be used by individual organizations to evaluate events that fall below the threshold for a national security.

Described another way, Consequence Prioritization considers threats greater than those addressable by standard cyber-hygiene and includes the consideration of events that go beyond a traditional continuity of operations (COOP) perspective.

Finally, Consequence Prioritization is most successful when organizations adopt a multi-disciplinary approach, engaging both cyber security and engineering expertise, as in-depth engineering perspectives are required to recognize and characterize and mitigate HCEs. Figure 1 provides a high-level overview of the prioritization process.

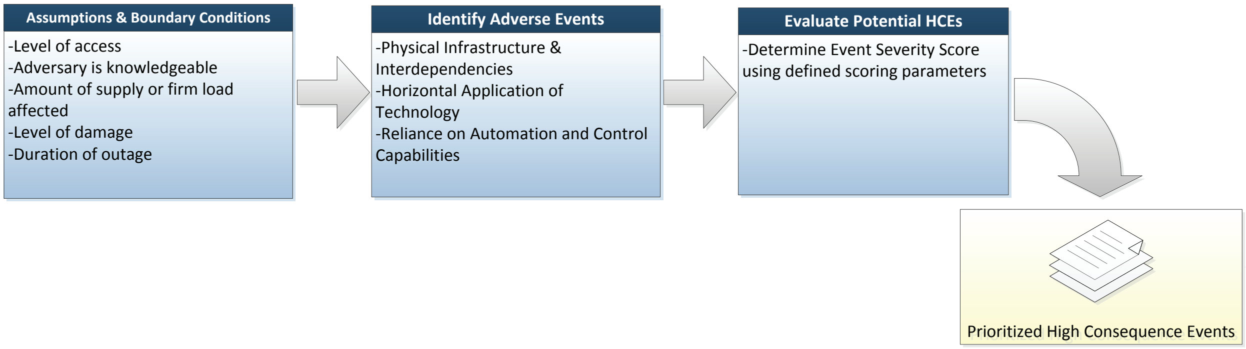
Assumptions & Boundary Conditions
-Level of access
-Adversary is knowledgeable
-Amount of supply or firm load affected
-Level of damage
-Duration of outage
Identify Adverse Events
-Physical Infrastructure & Interdependencies
-Horizontal Application of Technology
-Reliance on Automation and Control Capabilities
Evaluate Potential HCEs
-Determine Event Severity Score using defined scoring parameters
Prioritized High Consequence Events

Figure 1: CCE Prioritization Method Overview

2 Establish Assumptions and Boundaries

At the start of the Consequence Prioritization process, the team lead, with group input, should establish working assumptions and boundaries to better define the area or scale of interest. However, rather than focus on some aspects of likelihood of a cyber attack (such as intent*),* *Consequence Prioritization* is primarily concerned with the *impact* of a potential adverse event. All of these boundaries and assumptions should be agreed by all party members before initial potential HCE are identified. Some examples of assumptions and boundaries include the following:

Assumptions:

- **Access has been achieved**
  - Adversary has logical access, including all credentials, IP addresses, Firewall and application access, distribution management system (DMS) access, distributed control system (DCS) access, etc.

- **Adversary is knowledgeable**
  - They have an understanding of critical equipment and processes and all the knowledge to impact the system
  - They have access to the required equipment, engineering expertise, and tools

Boundaries:

- **Amount of supply or firm load affected**
  - Amount of supply (i.e., generation capacity) loss necessary to be considered significant which may vary from asset owner to asset owner

- **Level of damage**
  - Amount in monetary terms of damage necessary to impact company

- **Duration of outage**
  - Length of outage time necessary to impact customers and business.

3 Identify Adverse Events

Next the working group should generate the possible disruptive events that could occur within the following focus areas. As mentioned previously, a disruptive event is an event that would significantly inhibit an organization's ability to provide the critical services and functions deemed fundamental to their business mission.

3.1 Physical Infrastructure and Interdependencies

The first category of events to consider is those which impact physical infrastructure and interdependency areas. First consider the *physical elements* that are utilized in the performance of a defined process function. Example elements to consider within the electric sector may include generation, substation, transmission and distribution lines, control center facilities and other elements of the power system. Next, identify any interdependencies or choke points in the infrastructure. Specific examples may include:

Infrastructure Example:

Impacts to transmission lines near a power generation facility with intent to have multiple electric infrastructure impacts and power delivery choke points. The primary resulting impact of an attack on the transmission system is larger than just an impact on one line as there will be resulting power flow impacts across the transmission network, as well as impacting the underlying distribution system. Additional effects would impact the locally connected power generation facility and the loss of a delivery path for the power produced.

Methods of affecting transmission line infrastructure could include targeting the lines themselves, the insulators, towers, or the facilities where the transmission lines are interfaced. Transmission substations and switchyards contain a wide variety of electrical infrastructure elements that can be mis-operated to impact the energy flow on the transmission lines. These elements may include; breakers, switches, transformers, protection relays, voltage load tap change, capacitor banks, and circuit reclosers.

Interdependency Example:

For an electric utility with assets which include gas–fired electrical power generation station(s), a "choke point" example would be the natural gas delivery system, most typically a pipeline infrastructure. The power generation plants are dependent on the natural gas delivery system and/or natural gas supplier (in the natural gas supply chain, this describes the natural gas producer which can often be a company separate from the natural gas delivery/pipeline asset owner). The choke point could be targeted directly (delivery system or production system attack) or indirectly (delivery system or production system asset owner attack).

3.2 Horizontal Application of Technology

The second category of events to consider is those which impact a technology that is widely deployed, either within a system or across a geographic region. Additionally, the horizontal application of technology may refer to technology that supports a function performed by multiple organizations. Consider function-specific, widely-deployed ICS technologies belonging to the same technology vendor platform like: vendor-specific implementation model of PLC's, RTU's, protection relays, meters, etc. Often, single or even multiple instances/versions of these devices may be deployed throughout a critical infrastructure business enterprise for both geographically dispersed and localized asset models.

Another aspect to consider is the increased "depth" of a technology deployment; that is, there is an incentive to develop and adopt vendor solutions that integrate new and previously deployed, legacy technologies through common programming and monitoring applications. This broad and deep functional coverage within the systems is also attractive and valuable to a potential threat actor. Examples include:

Horizontal Application Example:

An electric utility may consolidate on a specific RTU vendor and a common communication protocol in an effort to drive consistency from site to site and reduce the level of system complexity for their field personnel. This creates an issue for the organization if a vulnerability is discovered in the communication protocol or in a specific vendor device that is deployed throughout a service territory. Corrective action to eliminate the vulnerability would be extremely time consuming if not impossible from a work force perspective.

From a distribution perspective, consider a smart meter worm that spreads throughout a smart meter infrastructure peer to peer mesh network exploiting the common protocol, common meter firmware, and leverages the built in capability to disconnect customer power. This creates an opportunity for an adversary to target consistency in architecture, protocols, devices, and provides a long deployment lifecycle for valuable exploits.

3.3 Reliance on Automation and Control Capabilities

The third category of events to consider is those which inhibit an organization's automated or control functions. Within the electric system there is a hunger for guaranteed reliability, and in order to achieve highly reliable delivery of power, there needs to be a system that can detect faults or system events and automatically respond or reconfigure in order to continue to deliver power to loads. This means that within the electric system there are systems and processes have been automated as they cannot be performed manually with the necessary real time response to ensure system reliability and safety.

Consider the various levels of the electric system. Power generation facilities, regardless of fuel type rely heavily on resource inputs like automated fuel management systems, feed water systems, water cooling systems, unit control systems, voltage regulation, and a wide variety of system protection controls that prevent damage or safety risks. An adversary can target any one of these automated systems individually or may recognize the redundancies in place and choose to misuse or manipulate multiple systems simultaneously.

Within the electric transmission and distribution systems, there are automated components designed to detect a line fault or physical condition that may have been caused by a down power line or pole, and automatically isolate the line through the operation of switches, relays, or breakers. In addition, other elements within the electric system may be switched in around the fault in order to deliver power to as many customers as possible, while responding to the line event. With an understanding of the recovery process, an adversary can send false data to these automated devices to cause mis-operations, or configure the devices in a manner so that they will mis-operate under normal conditions. The tendency for electric utilities to use common device types and communications infrastructures can make this a valid target for an adversary.

Electric Control Center environments contain entire systems that are designed to monitor and take action manual and automated across a wide footprint of the electric system. This may include hundreds or thousands of substation environments, dozens of power generation facilities, and hundreds of miles of transmission lines. The energy management systems located at control centers are used to keep the system in balance, but in the event of certain conditions, a control center operator may have to intercede, such as increasing generation to service load or shedding load to keep the system in a reliable state. An adversary with an understanding of this capability can target the energy management system components to initiate load shed events or manipulate data in a manner that makes an operator believe certain conditions exist that would require operator actions to prevent a wider scale outage. Specific examples include:

Automation and Control Example:

- Natural gas pipeline station volume and/or pressure control, compressor control, and station emergency shutdown sequencing which includes modern distributed safety systems (flame, gas, etc.).

- Any “real-time” remote monitoring and/or control of assets.
- Same day modifications to natural gas receipt and delivery volumes.
- Timely collection of accurate volume, gas constituent, and operational parameter data in a geographically dispersed set of system assets.
- Electric utility energy management systems (EMS) and energy load balancing systems.
- Power system area balancing through Automatic Generation Control and scheduling
- Power element maintenance ticketing and electronic-tagging systems
- Use of automatic load shedding schemes with in the EMS (Special Protection Schemes (SPS), Remedial Action Schemes(RAS))

4 Evaluate Potential High Consequence Events

4.1 Determine Event Severity

4.1.1 Calculate Impact Score

Use Table 1 to screen the adverse events through the first order effect of the evaluation methodology to begin to address the most impactful items. Each of the criteria is evaluated as a Likert scale, with most being evaluated as low, medium, and high (values 1, 3, and 5, respectively). This initial assessment is primarily concerned with evaluating the direct impact of an event.

It should be noted that *Attack Breadth* moves beyond the number of devices impacted, since this value also considers the additional resources needed for restoration, such as additional personnel or financial expenditures. For example, following a cyber attack targeting AMI, recovery efforts may be complicated by the quantity of field devices deployed.

> **Area Impacted:** Describes whether the impact of the attack scenario is geographically localized, or it impacts the entire system. Area Impacted is described as a loss of load (both firm and supply), which can be translated into a number of affected endpoints or accounts.
>
> **Duration:** Describes the length of outage.
>
> **Attack Breadth:** Describes the extent to which a targeted technology or system is deployed resulting in adverse operational effects. The greater the span of impacted systems, the more difficult the restoration following an adverse event.

Table 1: Impact Criteria

Criteria	Low	Medium	High
Area Impacted (Load or Customer Count)	Loss of failure to service firm load of less than 300 MW (or) load supply loss of MSC or 2,000 MW, whichever is lower.	Loss of failure to service firm load between 301 and 1,500 MW (or) load supply loss of between 2,000 MW (or MSC, whichever is lower) and 3,000 MW	Loss of failure to service firm load greater than 1,500 MW (or) load supply loss of greater than 3,000 MW
Duration	Return of all service in less than 1 day (inability to serve firm load) (or) supply outage for less than a week	Return to service in between 1 to 5 days (inability to serve firm load) (or) supply outage from 1 week to 1 month	Return to service in greater than or equal to 5 days (inability to serve firm load) (or) supply outage for greater than one month
Attack Breadth	Elements of the system are vulnerable to an exploit that is actively being attacked and causing operational effects, but recovery is possible using immediately available resources. These events are covered within the utility's recovery plan.	Multiple system elements have the potential to be or have been successfully attacked causing operational effects. Recovery is possible but requires additional resources (i.e., time, personnel, etc.) not immediately available.	Many system elements have been successfully attacked causing operational effects. Restoration is complicated by the dispersed deployment of devices or scale. Timeline for recovery is unknown.

4.1.2 Assess System Integrity Confidence

Use Table 3 to screen the adverse events based on System Integrity Confidence and assign a value of 1, 3, or 5 that correlates to low, medium, or high. Rather than focus on breadth of an attack, in some cases the system exploited may be central to the functionality of a critical service (i.e., the keep inside the castle) so that an organization cannot operate the same system again because the risk of a follow-on attack is too high. In contrast, an organization may have confidence in their ability to replace impacted systems or devices and return to normal functionality and operation.

System Integrity Confidence: Describes whether or not restoration and recovery efforts can restore system integrity with confidence following an adverse event (i.e., a system not operating as expected or intended, or, alternatively, malicious operation conducted by unauthorized users). One factor to consider is whether or not the initial attack propagates in multiple systems and therefore complicates restoration efforts. All of these may negatively impact an organization's confidence in their system following an adverse event.

Table 2: System Integrity Confidence Criteria

Criteria	Low	Medium	High
System Integrity – Asset Owner Confidence	Asset Owner has ability to restore and is confident in restoration integrity.	Asset Owner has knowledge to restore but does not have the resources (financial, time, personnel, etc.) to restore confidence in the system.	Asset Owner has ability to restore but is not confident of restoration integrity.

4.1.3 Assess Impact to Safety

Assess the potential impact to Safety using Table 4 to screen the adverse events. Assign a value of 0, 1, or 5 that correlates to none, low, or high impact to safety. This value considers only the direct impacts to safety and not safety issues that stem from extended outages.

Safety: Describes the potential impact on safety, including injuries requiring first aid or loss of life. For example: the power system outage resulting in health hazards or mortalities directly tied to the lack of available electric power.

Table 3: Safety Criteria

Criteria	None	Low	High
Safety	There is no risk to safety (no resulting injuries or death).	Low, but definite risk to safety, but only within the boundaries of "onsite."	There is a definite risk to safety "offsite." Beyond the boundary of the fence.

4.1.4 Assess Cost of Event

Assess the potential monetary impact using Table 6 to screen the adverse events. Assign a value of 0, 1, 3, or 5, which correlates to none, low, medium, or high cost of the event (including restoration).

> **Cost of Event (including restoration):** This criterion considers direct financial loss to the utility as a result of the failure scenario including restoration costs which is the cost to return the system to proper operation, not including any legal or other reparations as a result of the failure. It also includes secondary costs such as purchasing replacement power in order to meet the need. For example, an organization with long term contracts will be impacted less than one with short term agreements.

It should be noted that the cost of an event will be directly impacted by the size of an organization. That is, the cost of one event may be evaluated as low for one utility but may be evaluated as medium for a smaller utility due to the greater "balance sheet" impact for the smaller utility.,

Table 4: Cost of Event Criteria

Criteria	None	Low	Medium	High
Cost of Event	Inconsequential Event	The cost of the event is significant, but well within the availability of an organization to recover from.	There is significant cost for recovery and it will require **multiple years** for financial (balance sheet) recovery.	The cost of an event triggers a liquidity crisis and potential result in the bankruptcy of the organization.

4.2 Identify HCEs

Using the previously determined values, calculate the HCE Severity Score equation below:

$$\begin{aligned} HCE\ Severity &= \alpha(Area\ Impacted) + \beta(Duration) + \gamma(Attack\ Breadth) \\ &+ \delta(System\ Integrity) + \varepsilon(Safety) + \zeta(Cost) \end{aligned}$$

The weighting coefficient values (α, β, γ, and δ) were determined by engineering and electric sector SMEs. However, these values can, and should be altered to reflect the priorities of a utility or other organization (see Figure 2). For example, if an organization believes their primary concern is safety, then the value of ζ can be increased so that ζ has a value of three.

During the pilot study, the SME working group agreed upon the following weights.

$$\alpha = 3$$

$$\beta = 3$$

$$\gamma = 3$$

$$\delta = 2$$

$$\varepsilon = 2$$

$$\zeta = 1$$

In evaluating various example scenarios, the working group found that they were unable to answer every question for every scenario due to limited information. In these cases, some scenarios or events were evaluated as less significant due to their lower HCE Severity scores. In order to compare these values against the others in the sample set, all scores were first converted to percentages before being converted to percentiles.

Included in Table 5 is description of how the HCE Severity score is adjusted in the event of imperfect information. Note that the total number of impact points will change as a utility alters the weighting criteria. Using the values defined above, the SME working group evaluated each scenario against a total of 70 potential impact points, with the most significant events receiving higher scores. In cases where limited information required the elimination of a primary criterion (in this case duration, attack breadth, or area impacted), the total number of possible impact points decreased to 55.

For clarity, the second column was included to illustrate the elimination of some criteria (Attack Breadth, System Integrity, or Cost) for the example scenario included in Section 5 of this document. For each case, a percentage score was also calculated. While this system allows organizations to calculate HCE Severity scores in limited information situations, it should be noted that eliminating criteria also decreases the validity of the HCE Severity score for a given scenario.

Table 5: Example of readjusting scores based on imperfect information.

	Total Number of Impact Points	Example Scenario Scores	Percentage
No Criteria Eliminated	70	38	54%
One Primary Criterion Eliminated (i.e. Attack Breadth)	55	29	53%
One Secondary Criterion Eliminated (i.e. System Integrity)	60	32	53%
One Tertiary Criterion Eliminated (i.e. Cost)	65	35	54%

After calculating the HCE Severity Score, identify the top HCE for further evaluation in the CCE framework. If multiple HCEs are identified, some scenarios can be eliminated based on a pre-determined threshold, as depicted in Figure 2.

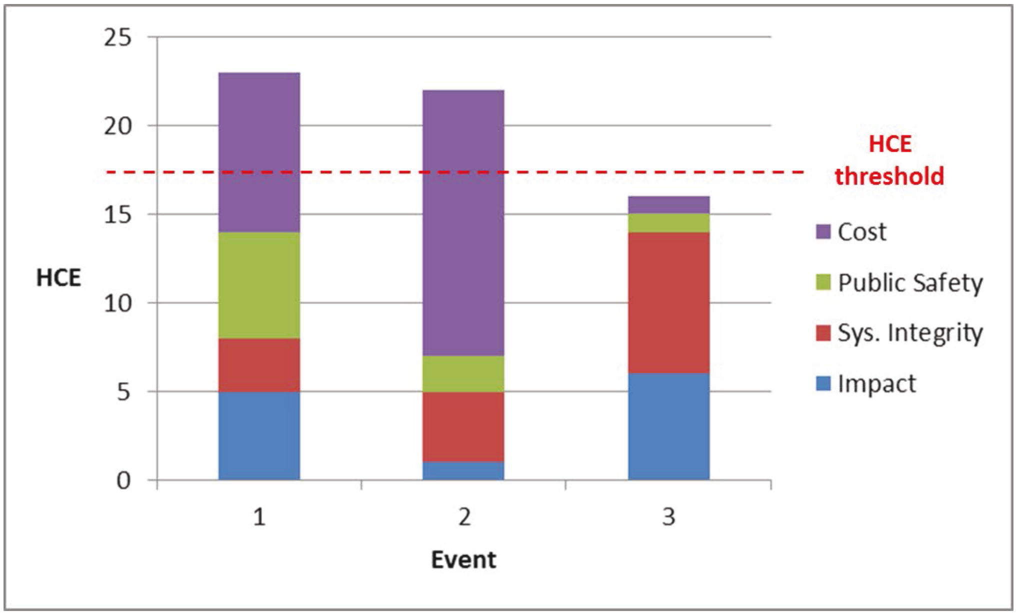

Figure 2: Example scenarios scored against a pre-determined threshold.

4.2.1 Role of the Group Lead in HCE Scoring

The group lead will act as a focal point for collecting and combining the scored scenarios from the SMEs. This individual should be knowledgeable in the scenario subject area(s) to lend guidance to questions that may arise during the scoring exercise.

Each potential HCE can receive different scores from the SMEs. In this event, the focal point has the discretion to combine the varying scores into a composite score. Regardless of the method chosen to combine the scores (i.e. median, average, most likely, etc.), the focal point should exercise care if any of the submitted scores are viewed as outliers. In this case, the focal point should request additional information from the SME(s) to better understand the rationale for the score, then make a decision about how to incorporate that score and rationale into the composite score.

It is important that all original documentation, including rationale, containing scenario scores be retained for future reference. The decisions made by the focal point should also be documented and retained for future reference.

5 Example Scenario Scoring

As an example of the scoring process, the following HCE has been assessed and scored below. The working group consulted with SMEs in order to assess the impact of this event. It should be noted that the event scored describes a system failure rather than the outcome of a cyber attack.

Scenario:

At the commissioning of an unspecified plant, a power interruption resulted in a loss of the control system. The plant had three combustion turbines (375 MW) and planned the construction of a 178 MW steam turbine to allow the plant to operate in combined cycle mode. As a result of the loss of power and resulting loss of the distributed control system (DCS), the auxiliary oil pump did not start after the trip. An emergency pump also did not start after the trip and all lube oil was lost during roll down. The damage to the steam turbine was extensive and included damage to the bearings, the rotor, the inter-stage seals and blade, which resulted in a loss of $12 million in repairs and $30 million dollars in lost income.[i]

Criteria	None	Low	Medium	High
Area Impacted		1 – While the scenario does not describe the area impacted, the working group assessed this event as low due to the ability of the utility to serve load via alternative means.		
Duration				5 – The working group believes that the resulting outage took more than a month to recover given the amount of time needed for the construction of the steam turbine.
Attack Breadth			3– As described, the working group believed that multiple systems could have been impacted (i.e., balance of plant (BOP) system, safety systems, etc.). Additionally, the impact scenario could be applied to other facilities of the utility.	
System Integrity Confidence			3- While there is limited information, this scenario would force the management of a utility to operate under the premise that their system integrity has been compromised (at least until a full cyber forensics assessment can be conducted).	
Safety		1 – There is a potential for a safety risk to onsite personnel.		
Cost of Event			3 – The scenario describes a financial loss of $42 million. The working group believes that this loss is	

Using the above scores, the HCE severity was calculated.

$$\begin{gathered} HCE\ Severity = \alpha(Area\ Impacted) + \beta(Duration) + \ \gamma(Attack\ Breadth) \\ + \delta(System\ Integrity) + \varepsilon(Safety) + \zeta(Cost) \end{gathered}$$

$$HCE\ Severity = 3(1) + 3(5) + 3(3) + 2(3) + 2(1) + 1(3) = 38$$

$$HCE\ Severity = \left(\frac{38}{70}\right) * 100 = 54\%$$

6 Acronyms

AMI	Advanced Metering Infrastructure
CCE	Consequence-driven Cyber-informed Engineering
COOP	Continuity of Operations
DCMS	Diverse Control and Monitoring System
DCS	Distributed Control System
DMS	Distribution Management System
EMS	Energy Management System
HCE	High Consequence Event
ICS	Industrial Control System
IP	Internet Protocol
IT	Information Technology
MSC	most severe contingency
MW	megawatt
PLC	Programmable Logic Controller
RAS	Remedial Action Schemes
RTU	Remote Terminal Unit
SPS	Special Protection Schemes

[i] Wallace Ebner, “Strategies for the Prevention of Turbine Lube Oil System Failures,” in *Proceedings of the ASME 2013 Power Conference*, July 29-August 1, 2013, Boston, MA.