# Consequence-driven Cyber-Informed Engineering (CCE):

A Targeting and Engineering Approach to Harden Critical Systems Against a Cyber-enabled Nuclear Security Event

R. S. ANDERSON

Idaho National Laboratory (INL)

Idaho Falls, USA

Email: Robert.anderson@inl.gov

A. BOCHMAN

Idaho National Laboratory (INL)

Idaho Falls, USA

Email: Andrew.Bochman@inl.gov

R. T. SMITH

Idaho National Laboratory (INL)

Idaho Falls, USA

Email: Robert.Smith@inl.gov

Abstract

Cyber Informed Engineering (CIE) was defined in IAEA CN-244-520 [1] as the inclusion of the cyber-attack and defence perspective (cybersecurity aspects) into the engineering process. It is the process by which engineering personnel are made aware of how their current actions impact the processes by which they architect and design systems. Decisions often do not consider attack tactics, techniques, and procedures (TTP) used by capable cyber adversaries. Consequence analysis and associated engineering mitigations are some of the most important elements within the CIE framework. Ensuring the most critical functions are available to perform as designed, when called upon, is vital. Idaho National Laboratory (INL) has created an operational process for performing cyber-informed consequence analysis and engineering mitigations. Consequence-driven Cyber-informed Engineering (CCE) is a cyber-defence concept that focuses on the highest consequence events from an engineering perspective so that resource-constrained organizations receive the greatest return on their security investments. The CCE process helps nuclear asset owners to: identify high-impact / high-consequence events if not already identified that could result in interruption of critical functions; analyse the infrastructure which could be subverted to enable those events; and develop specific mitigations to eliminate, or engineer out, unacceptable consequences of intentional mis-use or sabotage. An operational approach to CCE is provided.

## CCE AS AN ELEMENT oF CIE

Within the CIE framework, several elements should be considered when designing an engineered system that incorporates cyber-threat criteria. As previously written in IAEA CN-228-135 [2], CIE was described as the inclusion of cybersecurity aspects into the engineering process to reduce cyber risk throughout the entire project lifecycle. Historically, engineered or Operational Technology (OT) systems never considered threat as a design requirement. More often, it was handled as an after-thought once the system was ready for testing or installation. Usually only during testing phases of the project lifecycle would cybersecurity measures be considered, and only at the request of an Information Technology (IT) specialist who may (or may not) have been included as part of final verification. Otherwise, cybersecurity was not considered at all. Once the project has reached the testing phase, and beyond, it is much more difficult to provide effective cybersecurity mitigation, especially for OT systems. Simple and effective opportunities for robust cybersecurity measures are lost when not pursued during the earliest stages (phases) of the engineering lifecycle. Such missed opportunities may be the elimination of vulnerabilities during design or the reduction of complexities not required for the intended function(s).[[1]](#footnote-2) It is the intent of CIE to change the engineering and risk-management culture and process to inculcate cybersecurity as a fundamental engineering and operations principle. One of the best ways to do this early is to influence and encourage academia to include threat criteria (cybersecurity) to the engineering process.

One of the most important CIE elements is the protection of digital assets that perform the most critical functions. Although a nuclear security regime may include many critical functions, those functions, if not performed, could lead to unacceptable radiological consequences (URC) or high radiological consequences (HRC), as well as interrupt the operational asset or facility’s ability to perform its critical function, such as electricity generation, nuclear research, or reprocessing spent nuclear fuel. To reduce the probability of a URC or HRC in the nuclear sector, or similar effects for other critical infrastructure sectors, INL is leading a high-impact initiative to reprioritize the way high-consequence risk is viewed within the OT environment of a state’s most critical infrastructure. The CCE effort provides organizations with an operational process to examine their own environments for high-impact events/risks; identify implementation of key digital assets and components that facilitate that risk; illuminate specific, plausible cyber-attack paths to those digital devices; and develop concrete mitigations, protections, and tripwires to address the high-consequence risk. The protections put in place must remain effective as new threats and vulnerabilities are identified. CCE focuses on securing a specific “high value” subset of assets providing a high cost to benefit ratio for limited funding or resource limited organizations and as part of a defensive strategy. The remainder of this paper will describe the CCE process that can be utilized by any organization.

## Threat of CYBER-ATTACK properly assessed

In justifying this need for a paradigm shift in the engineering and security approach to designing critical infrastructure assets, it is important to first understand and accept the current threat of cyber-attack to critical operations. As the digital architecture of advanced operations has become increasingly complex, keeping cyber adversaries out of these systems has also become very difficult. The reality facing defenders in today’s digital environment is that if a well-resourced and expert cyber-capable adversary is intent on gaining access to a particular system or asset, it is only a matter of time and resources before access is achieved.

Fundamentally, OT suffers from a design basis “trust” relationship which assumes digital system separation can be maintained and protected against potential malicious exploitation. The reality, however, is the modern threat actor with cyber capabilities is constantly evolving and no separation method can be maintained. It is difficult to account for a threat that is co-adaptive (i.e., an intelligent human adversary) as the technology becomes the field of contest and can be used to defeat engineering design.

Cyber adversary access vectors are not limited to remote access over vulnerable networks. Supply chain and local access should be considered as other key vectors of adversary attack. For example, much effort and funding is put in to effecting “air gaps” to stop adversaries’ ingress to critical systems over network paths, but these same defences are often defeated through other access vectors such as an unwitting vendor with occasional access to key systems and devices beyond the air gap.

Given the threat of cyber-attack, asset owners and operators must consider (within their regulatory framework) how to avoid cyber-enabled sabotage, theft of sensitive information, or a “blended” attack that aides in the theft of nuclear or radioactive material even in an environment where the adversary has gained access to those systems. Engineering security controls and hardening systems to maintain critical operations in the face of adversary access justifies a shift to embrace CIE principles. If engineers can remove high impacts resulting from attempted cyber-enabled compromise through engineered systems, the cyber adversaries are left with little opportunity to cause critical mission ending events.

Current risk analysis does not typically account for indeterminant or mis-operation, (i.e., a digital asset behaving in a way for which it was not designed). Therefore, new risk analysis and design methodologies must be adopted to account for the co-adaptive nature of the hazard and devise potential mitigation strategies required for safe and secure operations. CCE, at its core, is an engineering approach that removes the “trust” assumption and fills existing cybersecurity gaps with a series of deterministically provable (i.e., demonstrably effective) defensive processes and procedures.

## PROCESS OVERVIEW

CCE is a guided methodology that leads an organization through critical steps required to protect its most essential functions and operations from the most capable cyber adversaries. Breaking CCE into its components:

* “Consequence-driven” signals an effort fully focused on minimizing high-consequence events (HCE) thereby protecting the organization’s most critical mission.
* “Cyber-informed” focuses the process on digital exposures or vulnerabilities associated with technology and related human tasks (e.g., patching, software upgrades, maintenance) that can be compromised to make systems operate in ways never intended or foreseen by their designer(s). Critical processes do not typically include cybersecurity as a fundamental design parameter and leave themselves susceptible to cyber-enabled compromise.
* “Engineering” refers to a systematic process followed to achieve the demonstrably effective protection against compromise. In addition, engineering and operations expertise and process knowledge is leveraged to create a more robust defensive strategy.

Before the CCE process can begin, preparation for engagement must be performed. As is the case with an effective incident response program, the preparation phase is most important and can take the longest amount of time and produce the most delays. Defining scope and negotiating data sharing and protection is very important. Identifying functional taxonomy must be developed while establishing a clear and compelling value proposition.

Consequence prioritization is the next phase and may be the most difficult to accomplish. It is the identification and evaluation of known and newly discovered HCE scenarios. Identifying the worst damage an adversary could impose on an organization can be challenging especially if there seems to be several such consequences identified or if consensus is not reached between the subject matter experts. This process may take days or weeks to accomplish.

A system of systems breakdown is the next phase to determine exactly what assets and processes are necessary to accomplish specific functions related to HCEs. All information pertaining to those systems must be known to identify the correct mitigation strategies. Identifying where key information is kept and who has access to it is also key to understanding how an adversary might build a campaign to achieve an HCE.

Once all the systems and assets have been identified, consequence-driven targeting can begin. Targeting expertise may be lacking within the organization, but it is imperative that effective adversarial analysis is performed to understand how an attacker may view the landscape. Attack trees can be an effective tool used in this phase. If the defenders can think like an attacker, identifying pathways and vulnerabilities may be easier. When adversarial targeting analysis is performed, it may lead to the production of sensitive or classified information that must be protected accordingly. After this analysis, it may be found that initial HCE scenarios identified may become less achievable, not feasible, or conversely, more within adversary reach than expected.

Finally, once the consequence-driven targeting analysis has been completed, effective defensive mitigations can be applied. In some cases, mitigation may require re-design if bolt-on solutions will not provide adequate protection.

### Pre-CCE Activities

One could argue whether the need for this entire (CCE) process is necessary. If we accept that only safety be considered against our worst HCE, we will be sorely lacking not to consider the threat component. Threat adds the complexity of never knowing with 100 percent confidence what the adversary will do next, nor the confidence to know that tomorrow another TTP may render existing protections useless. Therefore, it is imperative that the organization acknowledges the necessity of this type of process, and that limited resources are brought to bear to ensure all known analysis was considered to protect against HCEs. CCE process scope must be identified and agreements in place if third party technical authorities (TA) are brought in to help with analysis. Taxonomy must be refined, and knowledge base data must be accessible. Training should be provided on the CCE process to all involved so everyone understands the identified goals. Topical subject matter experts (SME) may be necessary during this process including operations and maintenance. Particular attention should be given to establishing an information security plan among the CCE team. Due to the nature of the analysis, organizations’ “crown jewels” systems will be considered. Keep in mind that outputs and reports from the process, if leaked externally, would provide the adversary with detailed roadmaps to effect HCEs.

### Phase 1 – Consequence Prioritization

At the start of the framework process, consequence prioritization enables organizations to define critical functions and services that allow the organization to accomplish its individual missions or goals. The goal is to identify potential disruptive events that would significantly inhibit an organization’s ability to provide the critical services and functions deemed fundamental to its mission. Consequence prioritization considers threats greater than those addressed by standard cyber-hygiene and includes the consideration of events that go beyond a traditional continuity of operations perspective. For example, losing the function of a nuclear power plant for one day may represent a bad business day, but losing a nuclear power plant for one month or more could have catastrophic effects. It is important to triage scenarios between business risk and mission-ending risk.

This phase may be the most important and the most difficult. Identifying HCE scenarios is not easy. Too many times, an organization will identify more than a dozen HCEs or critical functions and services, but this number is un-manageable with limited resources. Prioritization must be performed reducing this set down to a manageable set of scenarios that may pose a risk to nuclear security. When a dozen scenarios are identified, analysis and mitigation costs are too large and do not get funded. Within the nuclear sector, for example, the key in this phase could be to identify those events that could lead to public exposure to radiation or release of radioactive substances (nuclear security event), and then through a graded approach, less consequential events can be protected as there are less resources that can be applied. If this boundary is kept in mind, then limiting scenarios is achievable. Another potential HCE may be a blended cyber-physical attack by the use of digital technology to assist in the theft of nuclear or radioactive material from the compromise of security systems. Prioritization is most successful when organizations engage cross-functional teams that include IT and OT cybersecurity, operations, engineering, safety, and other relevant expertise. These types of skillsets are required to comprehensively recognize, characterize, and mitigate HCEs. The team lead, with group input, establishes and documents working assumptions and boundaries to better define the area or scale of interest.

Categories of events should be considered for this analysis. Physical infrastructure and interdependencies may be one of the first categories for consideration as these elements may be utilized in the performance of defined process functions. Example elements for the nuclear industry may be power systems, water supplies, or transportation. All interdependencies or choke points in the infrastructure must be identified, to include a thorough examination of supply chain issues.

A scoring matrix tool can be used to develop HCE criteria such as thresholds, casualty or safety, environmental, (outage) durations, cost, security, or emergency preparedness. Facilitation of these criteria helps keep discussions on track and should be limited to those absolutely necessary. Other criteria considerations may include whether the attack is geographically localized, regionalized, or global. Remember that cyber risk, unlike traditional risks from isolated equipment failure or human error, introduces a horizontal attack element that can cripple entire fleets of assets vice singular operations. SMEs should use the scoring matrix to prioritize and rank events with those meeting HCE thresholds. Manual vs. automatic functions should be considered. Scenarios should be no more than three to four sentence descriptions to include the end goal, the target, actions performed, and/or impacts. Final HCEs must be verified with senior decision makers.

### Phase 2 – System of Systems Breakdown

Taking a system of systems approach reveals actual hardware and software that performs the functions of interest that must be protected. Systems can be either analogue or digital, however, CCE focuses on digital assets and systems as these may be susceptible to cyber-attack. Translating final HCE scenarios into pictures, diagrams, drawings, or other visual aids help refine the taxonomy and build a common understanding. Functional taxonomy explains what is required to perform a critical function or service and points to elements that must be compromised to interrupt that critical function. Another task is to perform open-source reconnaissance on identified systems and assets including entity partners, collaborators, and vendor information. This task mimics what the adversary would do if they were to learn about the identified systems. This may reveal vulnerabilities, poor design practices, or poor documentation that may describe how to defeat certain functions, and a host of other potential liabilities.

Of course, the adversary does not have a level of systems and process knowledge comparable to what the defending organization has. Organizations should use this knowledge to their advantage when framing intelligent information requests. Furthermore, they should analyse documentation to pinpoint what is important and what is not. This phase may require many iterations before enough information has been collected to perform the next phase. The collected information should be used to populate the functional taxonomy. All elements of the populated taxonomy need to be well referenced and tagged, including SME comments and insights. Getting this phase right is vitally important, as this final taxonomy will be the source of information used in the next phase.

### Phase 3 – Consequence-driven Targeting

This phase requires an organization to turn its defensive mindset hat around and think like an attacker. How would an attacker manipulate and compromise systems in a manner that would allow for an HCE to occur? Digital assets can be manipulated through known or unknown vulnerabilities making them perform operations never intended by their designers within certain operational deployments. Or once elevated credentials have been captured, adversaries become authorized operators “living off the land” (i.e., using existing functionality) to manoeuvre, perform reconnaissance, prepare payloads, and perform other activities required to pursue their end goals.

To adequately understand and grasp the whole anatomy of an attack, one must visualize the final goal and work backwards through a kill chain or similar representation of the attacker steps so that areas of mitigation can be identified. Questions must be asked such as, what information is required to accomplish this scenario? Robust intelligence feeds become critical to understand the adversary capabilities, intent, and motivations including any newly identified TTPs. Items for consideration may include understanding the final HCE, the mechanism to accomplish this effect (conduct of operations), digital assets and system payloads necessary to accomplish such an event, access pathways, vulnerabilities, information locations, access required to execute system movement, and final execution of payload. Technical analysts must be cognizant of any key information exchanges between these systems, the loss of which to an adversary would result in an operational compromise, failure, or indeterminant state. Note that phase one focuses on the identification of high consequence events (scenarios), while phase three focuses on how the scenario is accomplished.

Once an adversarial “conduct of operations” (CONOPS) has been identified, SMEs must validate them. SMEs should revise and refine proposed CONOPS until all SMEs agree. Some HCE scenarios may be eliminated if it is determined that a particular CONOPS is not feasible. Once a CONOPS has been developed and validated, skills, resources, and capabilities required to perform such an operation must be determined. Information collected about the CONOPS must be presented to senior management for feedback and validation of scenarios and targets. This allows management to understand what might be possible and assign a risk factor. Some criteria used may be modified based upon business, operations, safety, security, emergency preparedness, political, or other such factors.

Once final CONOPS have been vetted internally with SMEs and approved as credible by management, this information should be shared with appropriate competent authorities and regulators to baseline potential adversarial possibilities that may be similar to other nuclear and radiological entities. Sharing this type of information can lead to more robust nuclear security.

### Phase 4 – Mitigations and Protections

The final phase is to put effective, defensive mitigations in place for those CONOPS’ identified vulnerabilities. Part of the management risk equation will be the costs associated with mitigation options. Some options may balance cost with effectiveness; however, the ultimate goal is to prevent an HCE from occurring. It may be necessary to re-design certain parts of the system to comply with recommended solutions. It is important to note that any re-design must go through standard engineering review processes to maintain the original function operation with no new vulnerabilities introduced due to re-design. SMEs must review all CONOPS and decide whether to secure key choke points or perform an exhaustive mitigation strategy throughout the entire system. If resident SMEs are not available, then a TA may be required to engage. Each mitigation or security measure should have a priority associated with it according to its function. It must be determined if the security measures selected is to deter, protect, detect, respond, delay, recover, or another attribute that would make sense for the system of interest to know if adequate defence has been identified. Security measures can be applied to either eliminate vulnerabilities or mitigate vulnerabilities. Decisions must be made as to how the effectiveness of each security measure will be determined and approved. Note, the CCE approach always prioritizes engineering solutions or “protection” over other forms of defence noted above, such as detect, respond, etc.

Regarding the value of re-engineering a digital system to remove the threat of function compromise, consider the following example. Within a nuclear power plant, a target for sabotage may be the turbine. Turbines use a vibration trip sensor to shut down the turbine safely in the event of an equipment failure or human error that could put the turbine into an unsafe operation. When considered from a cybersecurity perspective, if the adversary compromised the turbine controller, the adversary could defeat the safety vibration trip sensor. A simple way to engineer out this attack, or to implement a protection mitigation, would be to ensure that a non-digital safety trip is configured to function regardless of the digital turbine controller. This would ensure that safety is not defeated due to a cyber-attack before its intended purpose is required.

This type of CIE mitigation ensures that even if the advanced adversary manages to build and execute a cyber campaign to sabotage the turbine, the alternative engineered protection would eliminate the reliance of a single digital solution subject to cyber-attack and compromise to ensure safe operation.

Once decisions have been made on the final mitigation strategy, mitigations are implemented and validated against the CONOPS to determine if identified HCEs are no longer a concern. It is suggested to inform competent authorities of pertinent aspects of the HCE scenarios identified and their corresponding CONOPS. Intelligence agencies may provide additional feedback in the form of sensitive or classified information which must be appropriately received and protected.

## COMPLETEING THE CIE FRAMEWORK

Although we have just shown a successfully vetted process to identify and protect against HCEs involving digital technology, the rest of the CIE framework must be considered for a comprehensive cyber or computer security program. Concepts such as simplicity, accurate digital asset inventories, secure architecture, diversification, and the use of engineering controls are just a few of the remaining aspects for consideration when undertaking a comprehensive approach to cybersecurity. It is the hope of the authors that additional operational processes can be developed, such as CCE, to address other CIE framework elements. Engineering design analysis should always consider the adversarial threat when detailing specific designs, specifications, verification and validation testing, and recommendations, mitigations, and protections against the cyber-enabled threat. In some cases, CCE considerations may lead to a change in system, infrastructure, processes, or procedures to eliminate vulnerabilities or remove digital assets completely to mitigate HCEs.

## LESSONS LEARNED

INL has performed CCE at a few, key organizations within the electric and nuclear industries to date. Lessons learned from these pilot engagements are provided for improvement and awareness to those interested in applying the CCE process.

One of the most challenging aspects of the CCE pilot process was information sharing between the pertinent stakeholders. Those responsible for various aspects of the mission do not always communicate with each other on a regular basis and are not always able to coherently discuss what HCEs might be possible. Terminology is different, priorities are different, and facility knowledge is not always consistent based upon undocumented personal experiences. Half the battle is to locate the correct expertise and protect the shared information, while imparting collaboration between a variety of disciplines and backgrounds to reach a consensus that all can agree upon. Some information required for this process may not be resident and must be sought from a TA, vendor, or third party. Collaboration between these entities may also be required for some mitigation strategies.

Access vulnerabilities were observed primarily located within the supply chain outside of the organizations’ control but within their sphere of influence. Mitigations were focused on the need for robust third-party specifications and contracts.

## CONCLUSIONS

Although high functioning organizations apply cyber hygiene (e.g., conformance to cybersecurity standards, best practices, recurrent training) broadly across the enterprise, it is incumbent upon nuclear energy and other critical infrastructure organizations to go beyond basic cyber hygiene and protect against the highest consequence, catastrophic events such as unacceptable radiological consequences. To accomplish this, CCE can be applied to the nuclear industry in a manner that is structured, teachable, and repeatable. Although CCE has been presented here within a nuclear security framework, it can be applied to nearly any other digitally enabled industrial process or function to minimize the worst, HCEs.

REFERENCES

1. R. Anderson, V. Wright, C. Spirito, J. Rodriguez, Idaho National Laboratory – IAEA, “Cyber-Informed Engineering Defined”, IAEA CN-244-520, December 2016.
2. R. Anderson, J. Price, Idaho National Laboratory – IAEA, “Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology”, IAEA CN-228-135, June 2015.
3. M. Assante, T. Roxey, A. Bochman, CSIS – Center for Strategic & International Studies, The Case for Simplicity in Energy Infrastructure, October 2015.
4. R. Danzig, Center for a New American Security, Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America’s Cyber Dependencies, July 2014.
5. M. Assante, R. Lee, SANS Institute, The Industrial Control System Cyber Kill Chain, October 2015.
6. D. Sax, Bloomberg Businessweek, “In the Age of Cybercrime, the Best Insurance May Be Analog”, 10 March 2016.
7. Mission Support Center - Idaho National Laboratory, “Consequence Prioritization Process for Potential High Consequence Events (HCE)”, INL/EXT-16-40341, 31 October 2016.
8. A. Bochman, Harvard Business Review, “The End of Cybersecurity: No amount of investment in digital defences can protect critical systems from hackers. It’s time for a new strategy”, May 2018.
9. S. Freeman, C. St Michel, B. McClurg, Cybercore Integration Center - Idaho National Laboratory, “The Process of Consequence-driven Cyber-informed Engineering (CCE)”, INL/EXT-18-44814, 5 February 2018.
10. Mission Support Center – Idaho National Lab, “Consequence-driven Cyber-informed Engineering (CCE) Concept Paper”, INL/EXT-16-39212, 15 July 2016.
1. Roxey, Assante, Bochman, 2015, https://www.csis.org/analysis/case-simplicity-energy-infrastructure [↑](#footnote-ref-2)