SAND2024-06571R

Canada-US Blended Cyber-Physical Security Exercise: Final Report

Matthew K. Erdman, Michael T. Rowland, Andrew S. Hahn, Remengton Pierce, Anita M. Romero

September 2023

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

ACKNOWLEDGMENTS

The success of this project did not come from the efforts of any one person, but from a diverse team across multiple laboratories, organizations, and countries. Completion of this project would not have been successful without the efforts of Canadian Nuclear Laboratories, Bruce Power, Canadian Nuclear Security Administration, or Idaho National Laboratories. Also, success would not have been possible without the support from the primary US sponsor, NNSA NA-211 International Nuclear Security. The final count of people that had a role from Sandia National Laboratories alone was 49. Additionally, over 45 foreign partners participated in the execution, or observed the event.

Group Photo After the Canada-US Blended Cyber-Physical Security Exercise

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Canada-US Blended Cyber-Physical Exercise was a successful, first of its kind, multi-organization and multi-laboratory exercise that culminated years of complex system development and planning. The project aimed to answer three driving research questions,

- How do cyberattacks support malicious acts leading to theft or sabotage [at a nuclear site]?
- What are aspects of an effective combined cyber-physical response?
- How to evaluate effectiveness of that response?

Which derived the following primary objectives,

1. The May 2023 Cyber-Physical Exercise shall present a cyber-attack scenario that supports malicious acts leading to theft or sabotage.
2. The May 2023 Cyber-Physical Exercise shall define aspects of an effective combined cyber-physical response.
3. Analysis of the May 2023 Cyber-Physical Exercise shall evaluate the effectiveness of the incident response against pre-established exercise evaluation criteria.
4. Analysis of the May 2023 Cyber-Physical Exercise shall assess the effectiveness of the evaluation criteria itself.
5. Exercises shall be performed in a real-life environment.

The team believes these objectives were met, and the evidence will be presented in this report. Due to the novelty of the exercise, there were several lessons learned that will be presented in this report.

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ADS	Attack development system
CAS	Central alarm station
CDR	Critical design review
CLI	Command line interface
CMS	Communications management system
CSOC	Cyber security operations center
CNL	Canadian National Laboratories
ECS	Experiment control system
ELK	Elasticsearch, Logstash, and Kibana
ETE	Equipment test environment
HGU	Hand geometry unit
INL	Idaho National Laboratory
NNSA	National Nuclear Security Administration
NPP	Nuclear power plan
NSTC	Nuclear Security Technology Complex
OODA	Observe, orient, decide, act
ORR	Operational Readiness Review
OT	Operational technology
PDR	Preliminary Design Review
PPS	Physical protection system
SA&BS	Scripts, archive, and backup system
SNL	Sandia National Laboratories
SoS	System of systems
SDR	System Definition Review
SIEM	Security information and event management
SIR	System Integration Review
SOAR	Security Orchestration, Automation, and Response
SRR	System Requirements Review
SUT	System under test
SWR	Security work request
T(D)	Time of detection
T(CSD)	Time of cyberattack detection
WKID	Wisdom, knowledge, information, data

1. INTRODUCTION

The Canada-US Blended Cyber-Physical Exercise (referred to as the Blended Exercise here forward) was a successful, first of its kind, multi-organization and multi-laboratory exercise that culminated years of complex system development and planning. Though physical and cyber exercises are performed regularly at high security sites, it is the team's understanding that the Blended Exercise was the first exercise that fully incorporated a cyberattack exercise into a physical force-on-force exercise. Due to the novelty of the exercise, there were several lessons learned that will be presented in this report.

1.1. Project Journey

The original project plan titled "Project Plan for Blended Cyber-Physical Attack Exercise" and associated slide deck for Leadership of NNSA NA-20, Office of International Nuclear Security defined three driving research questions:

- How do cyberattacks support malicious acts leading to theft or sabotage [at a nuclear site]?
- What are aspects of an effective combined cyber-physical response?
- How to evaluate effectiveness of that response?

These questions defined the technical objectives to be completed for a successful event. Those objectives were defined as:

- To plan and construct credible attack vectors and a credible attack scenario.
- To determine the technology and process-based resources needed to support the development and execution of the exercise.
- To consider tools in use at NPPs to allow the following.
    - Planning the exercise participation and constructing the exercise flow.
    - Development of key performance indicators.
    - Preparation of materials to support the exercise.
- To develop tools to support and evaluate the exercise.

It was determined that if the team was successful in meeting the defined technical objectives that a risk informed, performance-based approach could be defined fulfilling a need for a better approach to assess performance for cyber-physical.

An issue that the team faced early in the project was managing the perception of what a realistic blended exercise would look like. This issue manifests itself due to movies and television inaccurately portraying cyberattacks, and how they lend the ability to perform a physical attack on a site. The most used example is the movie franchise Mission Impossible that portray cyberattacks coupled with physical attacks in a way that would not be realistic.

1.1.1. Project Requirements

The Blended Exercise derived requirements from the driving research questions defined previously. Out of the driving research questions, three original Level 0 requirements were derived with an additional two being added in December 2022. Those requirements were as follows:

6. The May 2023 Cyber-Physical Exercise shall present a cyber-attack scenario that supports malicious acts leading to theft or sabotage.

7. The May 2023 Cyber-Physical Exercise shall define aspects of an effective combined cyber-physical response.
8. Analysis of the May 2023 Cyber-Physical Exercise shall evaluate the effectiveness of the incident response against pre-established exercise evaluation criteria.
9. Analysis of the May 2023 Cyber-Physical Exercise shall assess the effectiveness of the evaluation criteria itself.
10. Exercises shall be performed in a real-life environment.

From these requirements, Sandia National Laboratories (SNL or Sandia) and Canadian Nuclear Laboratories (CNL) derived two separate sets of requirements. With CNL as the owner of the definition of an evaluation criteria with respect to the player actions, their requirements were heavily operator action dependent. With Sandia as the owner of the facilities and system development, their requirements were heavily system implementation and testing dependent. CNL's and Sandia's derived requirements can be found in the CNL "BlendedExercise" excel file and document "Canada-US Blended Cyber-Physical Exercise: Sandia National Laboratories Derived Requirements" respectively.

2. EXERCISE & PROJECT PLAN

The final draft version of the Project Plan was last updated in May 2022. This final plan defines two major exercises, the first being at CNL in Fredericton, Canada to examine the capabilities of the nuclear industry to recognize a cyberattack and the response to a cyber security incident in real-time using simulated Nuclear Power Plant (NPP) systems. The second being the Blended Exercise, referred to as the Signature Event and the blended cyber security incident response exercise. For the Blended Exercise, the original discussed contributions was for SNL to provide a host location and infrastructure, as well as the physical intrusion attackers. CNL was actioned to provide the key measurements and recordings.

Within the Project Plan, the main theory of the project was defined as, "Force-on-Force exercises involving cyber security can be evaluated with time-based performance metrics." This theory defined three hypotheses as follows:

1. Hypothesis 1: Blended Force-on-Force exercises can be evaluated using time-based performance metrics.
2. Hypothesis 2: There is a priority or importance in Time of Detection, T(D), in physical protection – comparative importance of T(D) and Time of Cyberattack Detection, T(CSD).
3. Hypothesis 3: Time scales can be made compatible between cyber security and physical protection.

Figure 2-1 and Figure 2-2 show the adversary task time for a physical protection system (PPS) response and the recovery parameters for a cyberattack response respectively. If the associated observations can be defined for both timelines and the actions needed to capture these observations and measure of times can be defined, then the original hypotheses can be proven.

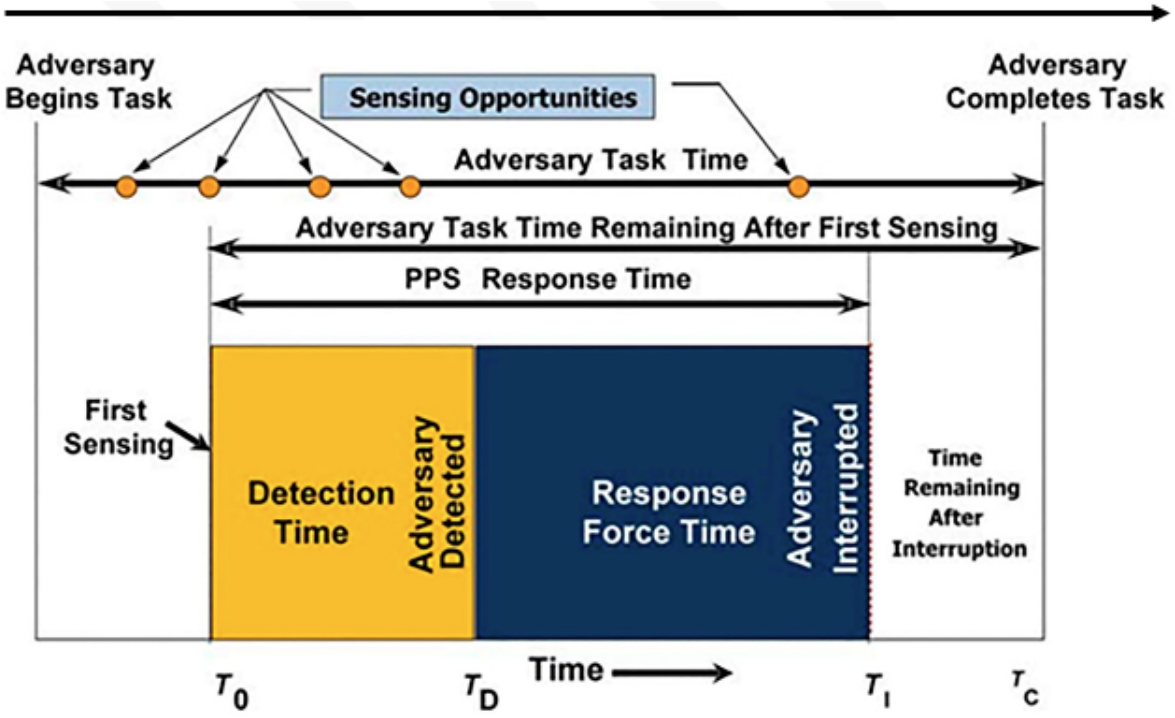


Figure 2-1. Adversary task time and PPS response

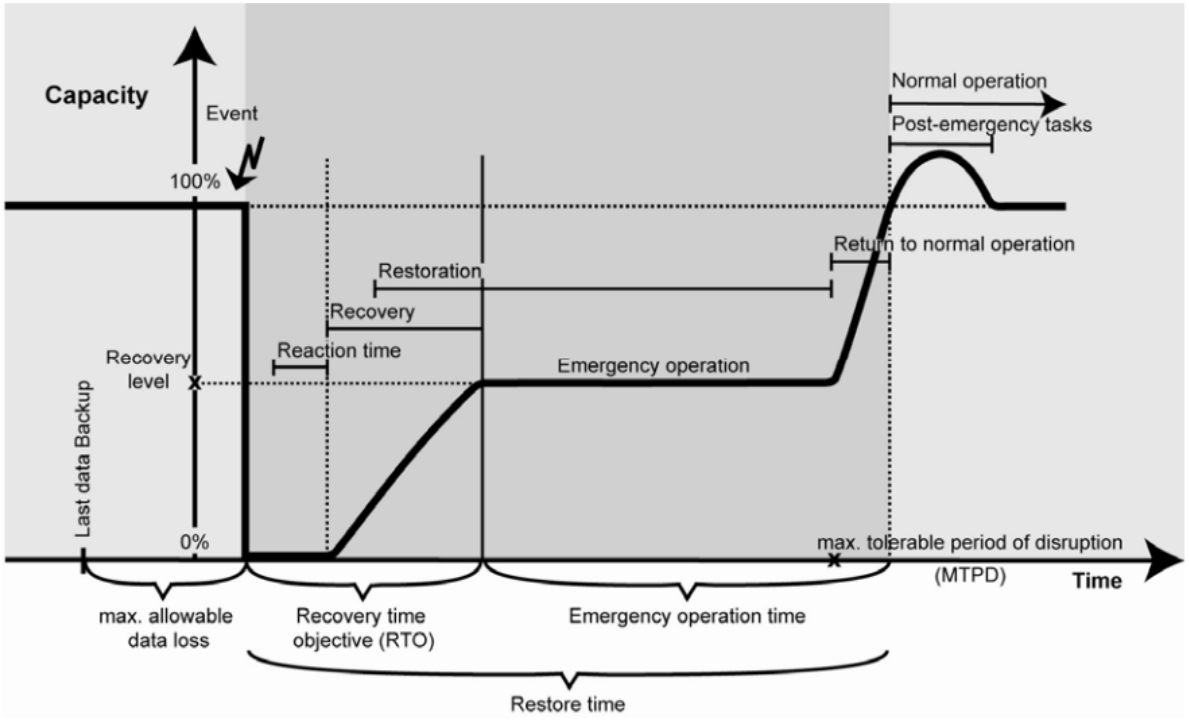


Figure 2-2. Recovery parameters as defined in the Project Plan (BSI 2009)

The project plan defined the original objectives to test the hypotheses as follows:

1. Perform a blended attack event to evaluate a methodology and platform to allow the following.
    a. Provide time-based criteria for completion of necessary tasks or activities by the cyber security operations center (CSOC) and central alarm station (CAS) operators.
    b. Establish criteria to evaluate the successful completion of each task or activity for both the CSOC and CAS.
    c. Advance best practices and technology with specific focus on the integration of physical protection and cyber security.
2. Cyber-attacks will be performed on The Nuclear Security Technology Complex (NSTC).
    a. PPS will be compromised, and that compromise may involve remote and local attacks on software, network, and/or hardware.
    b. Adversary observables and effects will be on the live system and performed by Idaho National Laboratory (INL);
    c. Elements of the PPS will be compromised during a limited scope performance test in October 2022.
    d. Given the importance of CSOC data, compromise of the CSOC is out of scope.
3. Physical attack will be conducted:
    a. Selection of scenarios may leverage computer animation (using SCRIBE3D) to show adversary progression in real-time. A reach goal is to make this interactive.

b. Physical Stimuli in real-time and space (smoke, vibration, rumble blocks) are being considered.

c. Occupational Health and Safety and worksite rules limit the level of physical stimuli, tactical attack/response that can be performed.

A project timeline with four phases was defined in the Project Plan as seen in Table 2-1.

Table 2-1. Outline of Events

Event	Date	Location	Phase
Project Kick Off Meeting	Oct 25th – 28th, 2021	SNL	Pre Phase 1
November Fredericton Trip	Dec 29th Nov – 3rd, 2021	CNL	
Cyber Exercise at CNL	Mar 7th – 10th, 2022	CNL	
Planning Meeting	May 2nd – 6th, 2022	SNL	Phase 1
Agreement on the Project Plan	May 31st, 2022	Virtual	
Review of CNL draft Tier 1, 2, and 3 Objectives	June 13th – 16th, 2022	Virtual	
Final prep meeting before the Dry Run	Oct 17th – 21st, 2022	SNL	Phase 2
Dry Run (redefined as February System Test)	Feb 20th – 24th, 2023	SNL	Phase 3
April System Test (added post Feb system test)	Apr 10th – 13th, 2023	SNL	
Dry Run (added post February System Test)	May 9th – 12th, 2023	SNL	Phase 4
Signature Event	May 15th – 19th, 2023	SNL	
Reporting and project closeout	May 20th – June 30th, 2023	Virtual	

3. TECHNICAL DEVELOPMENT

To test the hypotheses defined in Section 2, the team needed to define and develop a testing ecosystem. The ecosystem needed to have the ability to test and capture cyberattacks on equipment, then be able to reliably replay the captured attacks to a player. The two systems defined to capture the cyberattacks and replay them are called the Equipment Testing Environment (ETE) and the Experiment/Experimental Control System (ECS) respectively. The requirements of the ETE and ECS ecosystem are visually represented in Figure 3-1, Equipment Test Environment and Experiment control System Ecosystem.

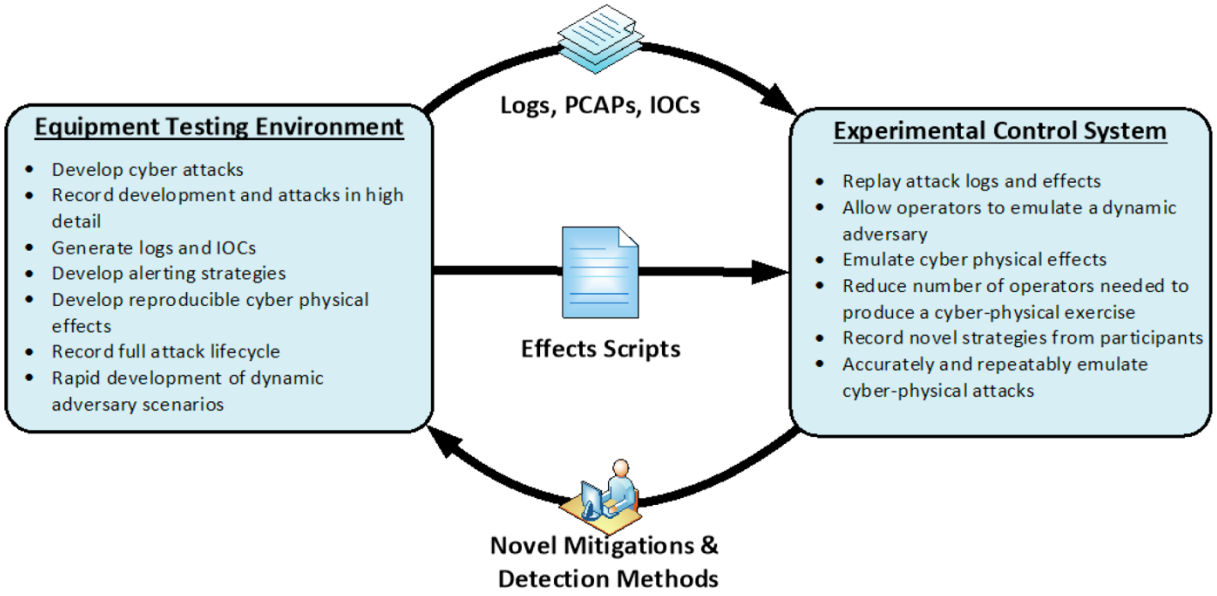


Figure 3-1. Equipment Test Environment and Experiment/Experimental Control System Ecosystem

3.1. Experiment Test Environment

The ETE is the system designed to capture traffic up and down stream of system under test (SUT) closest network switch shared with the attack development system (ADS). The communications management system (CMS) and ADS are connected to a control network that is isolated from the SUT. The security information event manager (SIEM) is connected in line to allow post processing of the traffic on the ETE network for processing of logs for development of CSOC response.

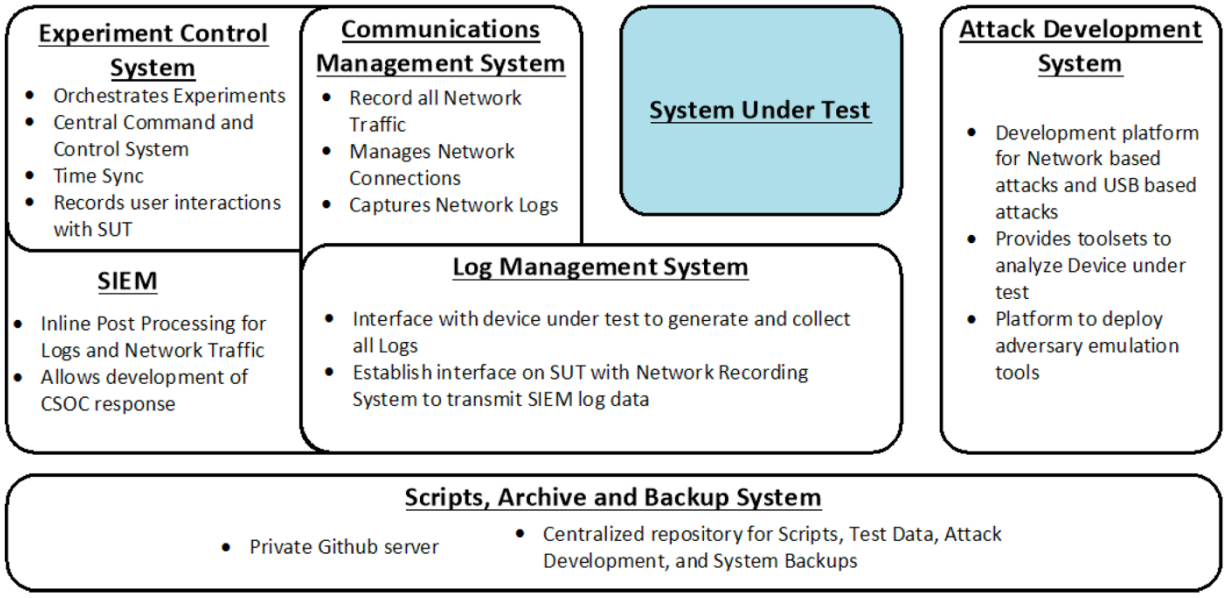


Figure 3-2. Equipment Testing Environment Block Diagram

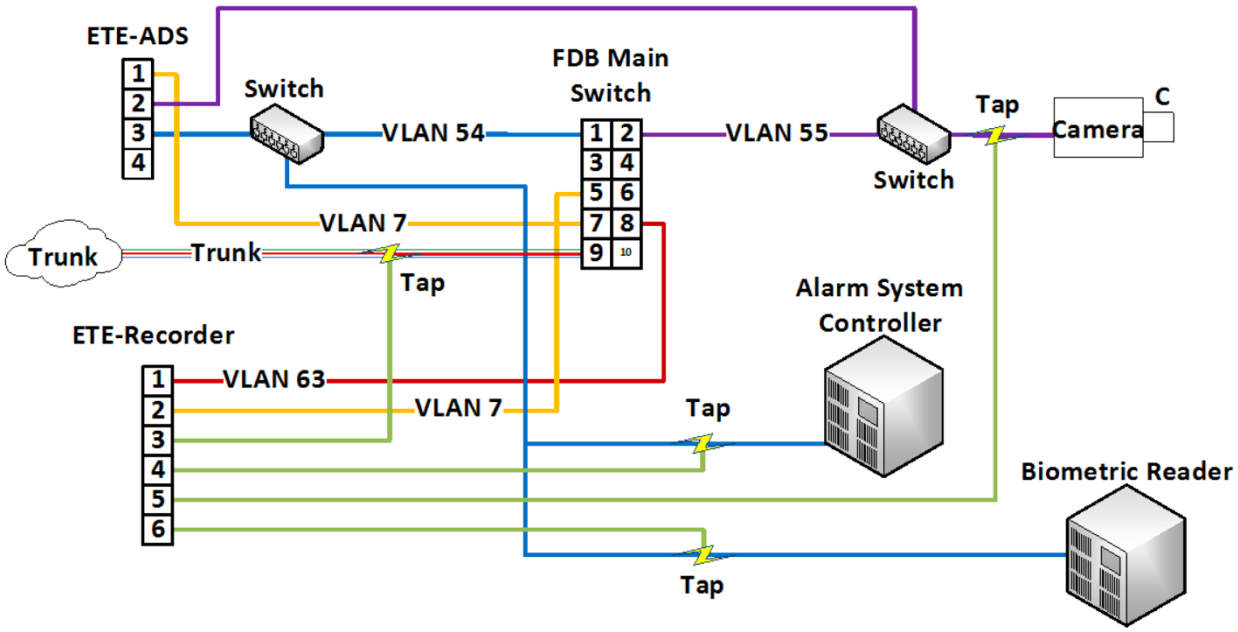


Figure 3-3. Equipment Testing Environment Line Diagram

3.2. Experiment Control System

The purpose of the Sandia ECS is to provide a holistic cyber-physical environment for experiments on the response of organizations and their personnel to cyber-physical blended attacks. These experiments seek to produce a better understanding of the evolution, impact, and manifestation of blended cyber-physical attacks. The intended result is the development of scientifically proven, results driven, defenses against complex cyber and cyber-physical attacks against critical infrastructure and sensitive environments.

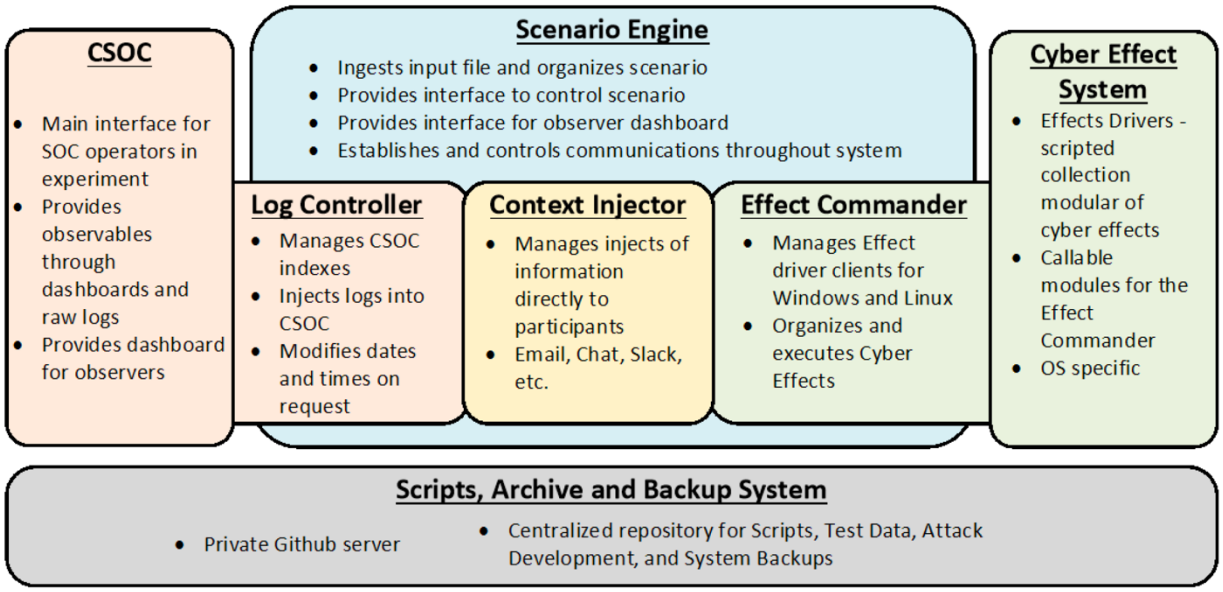


Figure 3-4. Experiment Control System Block Diagram

3.2.1. Scenario Engine

The Scenario Engine drives the ECS systems; it is the main orchestrator for the system. It reads an input file that contains the scenario and all permutations of the events based on relationships between scenes (parent/child). It provides an interface for the operator to control the scenario and choose branches of the event tree. It is also responsible for providing a dashboard or indicators for observers and the operator.

3.2.2. Log Controller

The Log Controller is subordinate to the Scenario Engine and provides control over the indexes of the SIEM and injects logs and observables into the SIEM. The Log Controller will receive generic log and alert messages from the Scenario Engine with relative dates and times, it will need to translate this to timestamps and inject these into the SIEM. It will also need to clear, reset, and manage indexes in the SIEM.

3.2.3. Context Injector

The context injector continues to be developed. This was not a critical component during the May exercise, but will prove to be very useful and as additional scenarios continue to be developed

3.2.4. Effects Commander

The Effects Commander is the interface between the Scenario Engine and the Cyber Effect System. Because the cyber effects happen across distributed systems, the Effects Commander must connect to and control Effects Agents on multiple operating systems. These Agents will use the cyber effects scripts of the Cyber Effect System at the command of the Scenario Engine. The Effects Commander will also be responsible for reporting to the Scenario Engine and thus the operator if there is an issue with a cyber effect agent. An Effects Agent can be any system from which effects will be launched. The Effects Commander will use remote command line interface (CLI) options such as SSH, PsExec, WMIC, etc. This will allow more flexibility when it concerns how and where cyber effects can be executed.

3.2.5. CSOC

The Cyber Security Operations Center is the main interface for participants and provides a SIEM interface for managing cyber alerts, network logs, and host logs. The CSOC also has access to PCAP traffic for further analysis. The CSOC uses an Elasticsearch, Logstash, and Kibana (ELK) stack based SIEM with plugins for the Log Controller to manage its indexes. It will be supplied with dashboards and alerts tailored to the needs of the scenario and experiment. Several accounts will be made on the CSOC machines for participants, administrators, the Log Controller, and Observers. These accounts will have different levels of access to the system information to allow information control.

3.2.6. Cyber Effect System

The Cyber Effect System is a collection of modules that interface with the Effects Commander and its Effects Drivers to produce cyber effects. These modules will need to be standardized in operation and arguments. They must also report success, errors, and failures to the Effect Drivers that call them.

3.2.7. Scripts, Archive, and Backup System (SA&BS)

The scripts, archive, and backup system (SA&BS) will provide the ECS a space to store data and backups. It must have some organization system to store the data transmitted to it. This will be the central repository for the ECS. Any component of the ECS may call upon the SA&BS to retrieve data for their operation.

4. RESULTS

Based on provided written and oral feedback from participants and observers, the consensus was the Blended Exercise was a success in execution and successful in supporting the project hypotheses as defined in the project plan.

1. Hypothesis 1: Blended Force-on-Force exercises can be evaluated using time-based performance metrics.
    a. This hypothesis was demonstrated via successfully applying a time-based application of the (Wisdom, Knowledge, Information, Data) WKID-Observe, Orient, Decide, Act (OODA) decision making processes to witness the cyber security team's and physical security team's ability to come to a timely decision on declaring a security incident. See Appendix A for further information on the WKID-OODA decision making process.
    b. WKID-OODA concepts have predictive power. During the blended exercise, key knowledge was not provided to or created by the cyber security players (i.e., CSOC team). During the exercise, WKID-OODA predicted that a cyber incident would not be called until the provision of the impact of the "unauthorized login" to the HGU event. This was captured in Table 4-1 at time 11:44 and Appendix D. This has lead to Bruce Power indicating interest in providing their comprehensive troubleshooting process and plans to SNL to evaluate using the WKID-OODA concepts.
2. Hypothesis 2: There is a priority or importance in Time of Detection, T(D), in physical protection – comparative importance of T(D) and Time of Cyberattack Detection, T(CSD).
    a. This hypothesis was demonstrated via the successful detection and decision-making process by the cyber security players. This enabled the cyber security players to inform the physical security players in a timely manner allowing them to initiate compensatory measures. This enabled the response force to remain effective even with compromised security systems.
    b. Security culture was a critical factor in determining T(D), which was approximately 75 minutes ahead of T(CSD) for the exercise. T(D) < T(CSD) also supported the WKID-OODA concepts, as the physical security players ascertained the understanding (or knowledge) of the event before the cybersecurity players. This allowed for the physical protection players to make good decisions and undertake actions (i.e., wisdom) before the cybersecurity players.
    c. T(D) occurred prior to the initiation of the blended attack. Therefore, the physical protection response was sufficient to defend the attack. Given the time/duration limits, further investigation would be necessary to determine costs of sustaining a heightened security posture.
3. Hypothesis 3: Time scales can be made compatible between cyber security and physical protection.
    a. This hypothesis was demonstrated via the successful execution of the Blended Exercise that demonstrated a cyberattack and how it enabled a physical attack on a mock nuclear site.
    b. Resources impact the time compatibility of the time scales. During the debrief, it was noted that physical security provides protection and monitoring on 24/7 basis, with

an additional work crew (i.e., shift) that allows for flexibility during security events. Cybersecurity personnel are only provided during standard business hours, Monday to Friday, with limited additional staff that could support event investigations and response.

From what the team understands, this was a first of its kind exercise and its success is a representation of the development team's ability to adapt and overcome challenges by coming up with solutions to issues quickly and minimizing the development of more issues by correctly accounting for risks. Part of the success of the exercise was due to the team's ability to define a realistic scenario and accurately predict when anticipated actions of the players should be expected based on the inputs provided to them from the system. Input from the controllers to the players to take major actions was minimal, showing the team diligently reviewed the scenario to ensure it was realistic, flexible, and well planned.

The successful progression of the scenario wouldn't have been possible without a reliable ECS that provided a reliable input to the players to act on. The fact that the exercise was as successful as it was, proves the ETE/ECS ecosystem was developed to an adequate level and can reliably perform as expected.

Also, the success of the exercise wouldn't have been possible without a realistic environment that was emulated by the Simulation Cell. Without the Simulation Cell, the physical security players would not have been in a realistic environment, discrediting the collected data on their actions.

The Observer Area and the content provided during the exercise provided an environment for observers to fully appreciate the actions the players were taking, lending to observer experience success. The space was quickly adapted to the state it was in during the exercise, allowing for many observers, including virtual, to experience the exercise.

4.1. Scenario Timeline with Notable Player Actions

Following is a rough timeline of events for the exercise with corresponding MSEL numbers and notable actions taken by the players. At times, player actions to MSEL events did not directly correlate with a specific MSEL event, which is noted in the table with an N/A in the MSEL event. This time correlated information was collected via the PREP messaging between controllers. The Prep

Table 4-1. Timeline of Events

Time (HH:MM)	MSEL	MSEL Event	Notes on Player Actions
09:30	5,6, and 7	CAS and CSOC simulated shift turnover	
09:35	8	Technician performs security work request (SWR) on non-functioning camera	
09:51	9	Vendor non-conformance report provided to players	
10:01	10	RSE review logs associated with non-conformance report in CAS	
10:13	N/A	N/A	CSOC confirmed no alerts from non-conformance report and reported back to RSE
Act I – Biometric Attack			
10:15	11	Initiate biometric attack. Alert associated to adversary removing contractor access is sent to the CSOC Note: Alert to CSOC delayed until 10:22	CSOC contacted RSE immediately of alert since associated to non-conformance report, suggested to check personnel accounting logs
10:22	12	Contractor denied access	
10:25	13	Contractor directed to get card reprogramed. Shortly after alert associated to adversary re-adding the contractor to system is sent to the CSOC Note: Alert to CSOC received 10:30	
10:29	14	Contractor gains access	

Time (HH:MM)	MSEL	MSEL Event	Notes on Player Actions
10:39	15	Alert associated to adversary adding access for an adversary team member is sent to CSOC. Adversary gains access to site Note: Alert to CSOC received 10:41	
10:45	16	RSE review logs again in CAS	CAS reviewed video and work orders to confirm or deny physical access granted to HGU management system
10:47	N/A	N/A	CSOC informed CISO that a CSIRT may be stood up depending on further findings from RSE
11:00	19	Fuel shipment at site	
11:10	N/A	N/A	CAS informed RSE that no one had physical access to HGU management system based on access logs and work orders RSE in turn provided information to CSOC CAS continued to investigate to see if video existed to verify confirmed or denied access to HGU management system
Act II – Camera Attack			
11:15	17	Camera reboot/reset	
11:21	N/A	N/A	CAS reviewed video at ECP to assess individual that entered associated to HGU alert timing
11:44	N/A	N/A	CSOC initiated an incident

Time (HH:MM)	MSEL	MSEL Event	Notes on Player Actions
11:47	N/A	N/A	CAS reviewed video of material receiving action to see if individual seen at ECP is also at the material receiving area during the material transfer
12:07	N/A	N/A	CSOC called for CSIRT meeting Meeting started at 12:12 after arranging POC's
12:37	Pause for Lunch		
13:19	Resume Exercise		
13:26	18	Camera IP change Note: Alert to CSOC received 13:31	
13:33	N/A	N/A	CAS locked down ECP and initiated 100% personnel accountability
13:35	N/A	N/A	LAN Turtle is 'found' by technicians/RSE
13:40	N/A	N/A	CSIRT Meeting
14:06	N/A	N/A	CAS requested additional patrols
14:20	N/A	N/A	CSOC inquired with CAS about physical access to camera maintenance workstation
14:47	N/A	N/A	CSOC identified illegitimate traffic associated to attack CAS heightened visual tracking of area around Mock-MRA
14:50	21 & 22	Adversary attacks the biometric devices and cameras to prepare for physical intrusion	

Time (HH:MM)	MSEL	MSEL Event	Notes on Player Actions
15:00	23, 24, 25, 26, 27	Adversary breaches the ECP, breaches the exterior door to the MMRA, and breaches the interior door to the MMRA, but is stopped prior to the entry into the MMRA	

4.2. Discussion

A key part of this exercise was that both Bruce Power physical protection and cyber security personnel were "blind" participants in the blended attack exercise to evaluate their response performance. Since, only one exercise and scenario was conducted, these initial and anecdotal results provide insights into the challenges to site response to blended attacks and a potential value of concepts such as WKID-OODA Loop to provide an intuitive structure to assist in planning, development, conduct, and analysis of future exercises. See Appendix B for additional context on the WIKD-OODA loop concept.

In the exercise, the cyber security and physical protection personnel were challenged by the ambiguity of the information and the incomplete situational awareness. One of the key lessons learned was the importance of concepts that could be used to predict challenging tasks of personnel prior to the exercise. SNL researchers suggested the WKID-OODA concept to support the project plan hypotheses, specifically hypothesis 1 and 2. WKID is a concept that is the overarching functional objective (i.e., what needs to be achieved?). It begins with data from digital technology and ends with wisdom which is the making of good decisions or undertaking good actions. OODA (Observe-Orient-Decide-Act) provides a means for the performance requirements (i.e., how quickly and how well does a functional objective need to be achieved?). See Appendix A and B for additional context on the WIKD-OODA loop concept.

Due to the MSEL design and the differences in location, from Bruce Power's site, there was no capability to evaluate the timing and performance of the personnel's OODA loops. This was due to the following reason:

1. Only one scenario was conducted which is insufficient to draw general conclusions, therefore all results are anecdotal and provide potential opportunities for further investigation.
2. MSEL design needed to consider time compression, 4-6 hours of exercise, including breaking for lunch, which does not reflect typical progression of cyber-attacks that target sensitive networks.
3. MSEL design was deterministic, whereby adversary behaviors and actions were unchangeable. The participants did not impact adversary behavior.
4. RSE as an "actor" reduced challenges for the sense-making loop, as the RSE already knew the desired actions and decisions (i.e., Wisdom). The RSE is a key role that would provide greater insight into the challenges in sense-making.

However, for there were some key insights from the exercise which are:

1. WKID concept may have predictive power
2. Security Culture was a significant differentiator in the performance of physical protection vs. cybersecurity
3. WKID-OODA may provide insights into development of exercises and guidance to support allocations of resources for people, process, and technology

The use of the WKID concept, especially for the observer experience, was a beneficial way to convey the challenges of blended attack response, but also the differences in the clarity and completeness of the data and information before knowledge and wisdom could be achieved. The physical protection staff performed well and reacted quickly due to lower thresholds for clarity and completeness. The CSOC team were challenged to perform sense-making loops, requiring an incredible effort and time, that they were unable to complete due to time constraints.

While not definitive, the WKID-OODA concept confirmed the predictions during the observer experience were correct for staff, like the CSOC, that has to meet high standards before calling an event. Additionally, technology can be both an aid and a detriment. The specific words of the alert were continually displayed perhaps biasing the CSOC staff that the unusual account login was not very impactful as it was likely seen by CSOC staff on multiple systems at their facilities. Pairing the wording with impacts would require more than generic information, leading to technology providing knowledge, or information with a potential to upgrade to knowledge more easily.

However, the greater knowledge that is provided by the CSOC creates potential for error, especially for false negatives or false positives. Security culture may have a role to play in determining this balance as the physical protection staff was able to act without conducting a sense-making loop. Sustainment of the incident management and response for a long duration would eventually require the physical protection staff to meet the same WKID thresholds, but compensatory actions were immediately taken to reduce the risk, but as expected, an increase of costs.

Additionally, the CSOC manager indicated that the WKID-OODA concepts reflected what he was attempting to do in an ad-hoc manner. There have been several correspondences about how to leverage these concepts to improve their people, processes, and technology.

OODA loop evaluations were not completed due to the aforementioned constraints. However, performance requirements (When is something needed to be completed? How reliably?) are tremendously important especially given the long delay in effective response. For performance requirements, these need to be exercised with all components in close to identical environments. Table top exercises will be insufficient in challenging the performance requirements as they eliminate technology and focus on process and people. However, the scenario's determinism, structure, and time constraints removed potential investigation of performance requirements. These requirements are critical for informing the strategy for implementing an effective incident response capability through strategic allocation of resources, technology design and implementation, establishment and maintenance of organizational processes, and development and coordination of staff.

4.3. Possible Next Steps

Following are some possible next steps based on the findings of the exercise.

4.3.1. WKID-OODA in Site Procedure Development

WKID-OODA concepts can inform strategic investments in process, people, and technology. For example, technology can provide Data, Information, Knowledge in real-time but requires extensive

development time and funding, sufficient coverage of monitored assets and systems, and tuning. Processes can consist of procedural, checklist-type, playbooks or general guidance, such as Bruce Power's complex troubleshooting plan. Playbooks simplify the interactions between people and technology and support consistent performance. General guidance places significant reliance on people (i.e., staff) to apply their knowledge, skills, and abilities in an effective way, but this is highly dependent on the individual or the organizations training and qualification programs.

WKID-OODA concepts in conjunction with a partner's people, processes, and technology can generate scenarios/MSEL that specifically target desired areas of a partner's incident response. WKID-OODA concepts may be predictive to allow for specific events within the scenario that exercise people, processes, and technology in a specific manner, in line with the partner's needs The results of the exercise can be evaluated to provide suggestions on how to optimize their incident response (e.g., people, process, technology).

4.3.2. Scenario Characterization

It was observed that there is an opportunity to further expand on the scenario development process. The ECS has additional capabilities that were not utilized in the scenario. The potential variations could include:

1. Provision of initial event(s) to the physical security players. The initial detection event in the (Teixeira, et al. 2015)original scenario was a Cyber SOC alert that was communicated to the physical security players via the RSE.
2. Provision or removal of additional event(s) to the cyber security players. Technology support for WKID can be controlled. Alarms to the cyber SOC can be Data, Information, or Wisdom.
3. Variation and permutations of scenarios that consider changes in adversary behavior based on player responses. Adversary behavior can be changed to become stealthier or noisier (i.e., less or more detectable). The ECS can provide for a non-linear branched (e.g., tree) scenario that allows for more complex and realistic exercise scenarios.

One possible approach is to further characterize scenarios based on the knowledge of the systems affected and if there is a procedure to mitigate the threat. With this approach, the attacks can be mapped to better understand how challenging a scenario is. If future engagements can focus on a stepped approach on how challenging the scenario is, the participating partner can gain substantial knowledge on where processes need development and where knowledge can be gained on systems. This can be visualized with the cyber-physical attack space as described in Teixeira, et al.

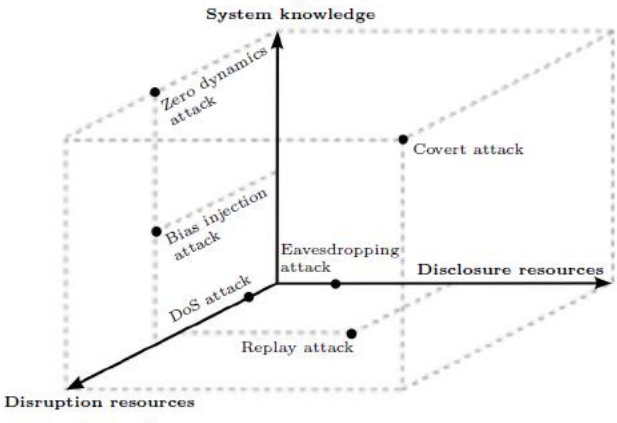


Figure 4-1. The Cyber-Physical Attack Space (Teixeira, et al. 2015)

An example from the blended exercise, was the team leveraged a LAN turtle and USB Rubber Ducky as the disruption and disclosure resources; and an active insider with considerable system knowledge. While there are considerable scenario permutations that can be developed with these resources and system knowledge, changes in system knowledge, disruptive and disclosure resources would provide significant flexibility and diversity in exercises thereby enhancing the value to partners and to understanding of necessary elements to effective response to diverse cyber-physical attacks.

4.3.3. WKID-OODA Loop to Develop MSEL

It was witnessed at the event that the WKID-OODA loop is has predictive power, structured thinking, and pre-analysis of what the expected outcome will be. In future exercises this tool can be used to structure the MSEL of the exercise. In this approach, expected actions can be defined as either Good, Neutral, or Bad with the following definitions.

- Good – make sense making loops, upgrade former knowledge to wisdom in a timely manner
- Neutral – not enough information, so they have to do a foraging loop. They have to pause to make sense of the information
- Bad – make a bad decision, upgrade former knowledge but come to the wrong decision.

WKID-OODA concepts can inform strategic investments in process, people, and technology. For example, technology can provide Data, Information, Knowledge in real-time but requires extensive development time and funding, sufficient coverage of monitored assets and systems, and tuning. Processes can consist of procedural, checklist-type, playbooks or general guidance, such as Bruce Power's complex troubleshooting plan. Playbooks simplify the interactions between people and technology and support consistent performance. General guidance places significant reliance on people (i.e., staff) to apply their knowledge, skills, and abilities in an effective way, but this is highly dependent on the individual or the organizations training and qualification programs.

WKID-OODA concepts in conjunction with a partner's people, processes, and technology can generate scenarios/MSEL that specifically target desired areas of a partner's incident response. WKID-OODA concepts may be predictive to allow for specific events within the scenario that exercise people, processes, and technology in a specific manner, in line with the partner's needs The results of the exercise can be evaluated to provide suggestions on how to optimize their incident response (e.g., people, process, technology).

4.3.4. ECS Development

The ECS allows significant capabilities but has significant room for expansion. The context injector is not yet developed and would allow the operators to inject emails and documents directly to the players without the need for additional actors or controllers to do so. The log system currently only works with the Elasticsearch because it is opensource, but many players are more familiar with Splunk. The connection to Splunk is entirely possible, the only barrier is the cost of Splunk licenses and additional development time. The long-play system for logs that provided background log noise for realism needs to be revamped as it takes too much time for it to load and start playing the larger +4 Gb log data files. Lastly, the effects system should have more effects developed for it. So far only the camera and biometric systems are under its control, but it has vast capabilities to provide very interesting effects. Though this will require more cyberattack development with the ETE to find realistic effects to emulate.

One of the findings from the exercise was that the ECS required experienced operators. While the interface is very effective technically, it was not intuitive enough to operate visually by someone without experience with command line-based systems. Improving the interface will require significant development time and cost, which is why it wasn't a top priority during development. Given more time and development resources, the ECS could be developed with an interface that would require minimal training to operate.

Development of the ECS will allow future exercises to be run with as little as one person with even further development getting the system to a state that it runs with automatic injections that are either time dependent or event dependent with those events being variable based on player actions. To get to this state further substantial technical development will be necessary. This will require player interfaces and security orchestration, automation, and response (SOAR) system capabilities to be introduced. An operational technology (OT) SOAR is not technically deployable in the industry yet, but the ECS can be ready to experiment, exercise, and develop the capability with operators when it is.

Next steps to completely automate the ECS include implementation of time dependent injections. To develop event driven injections, implementation of decision trees will need to be added to the system. Further development on the decision process will need to be done to develop a clear development path on event and decision dependent injections.

5. LESSONS LEARNED

Though the Blended Exercise and project was deemed a success, there are lessons learned to make similar exercises, projects, and future work on the Blended Exercise systems be more successful. The overall theme of the lessons learned is that from the planning phase to the execution phase, there was a lack in structure in the execution of the project. Though it will not solve all the problems specified in this Lessons Learned section, implementation of NASA's systems engineering engine (Shishko 2007) will provide a framework to approach development, testing, and validation of a complex system of system (SoS). As visually represented in Figure 5-1, the systems engineering engine defines the system design, product realization, and technical management process. This process should be implemented for every system within a complex SoS setting to better flow down requirements from higher levels and to flow up realized products to become incorporated into the overall system.

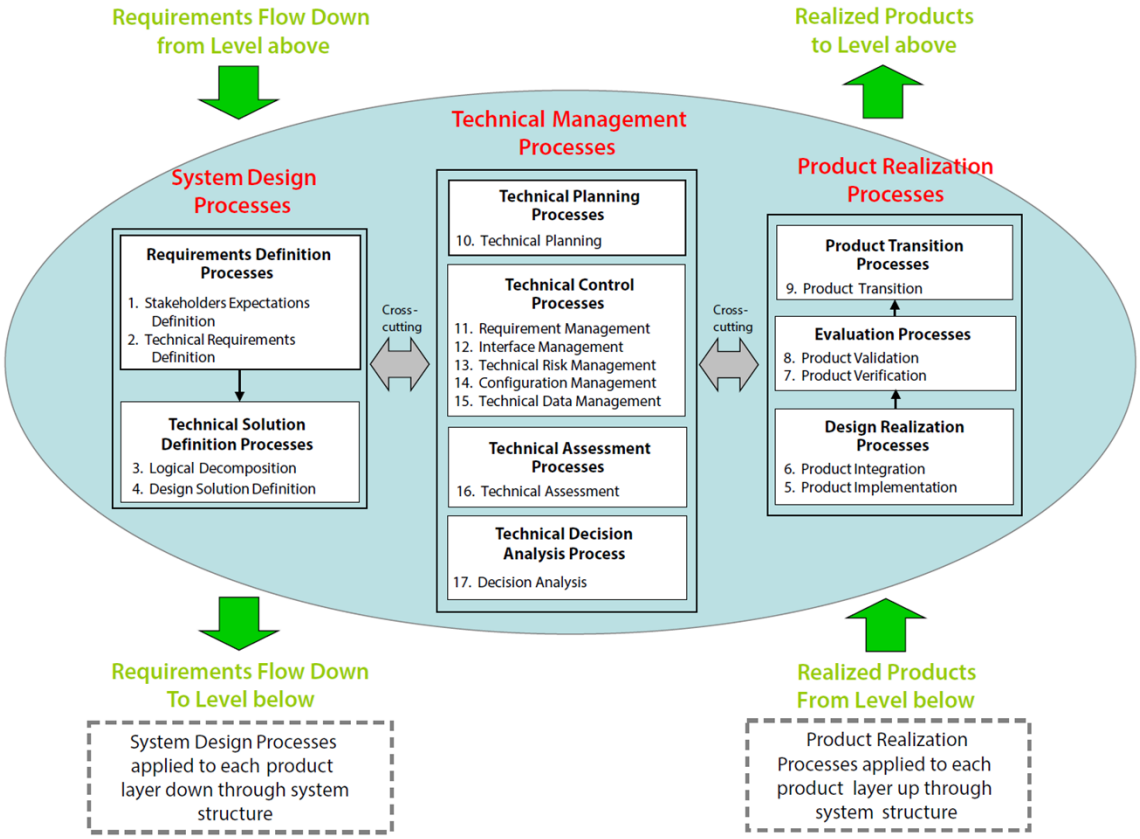
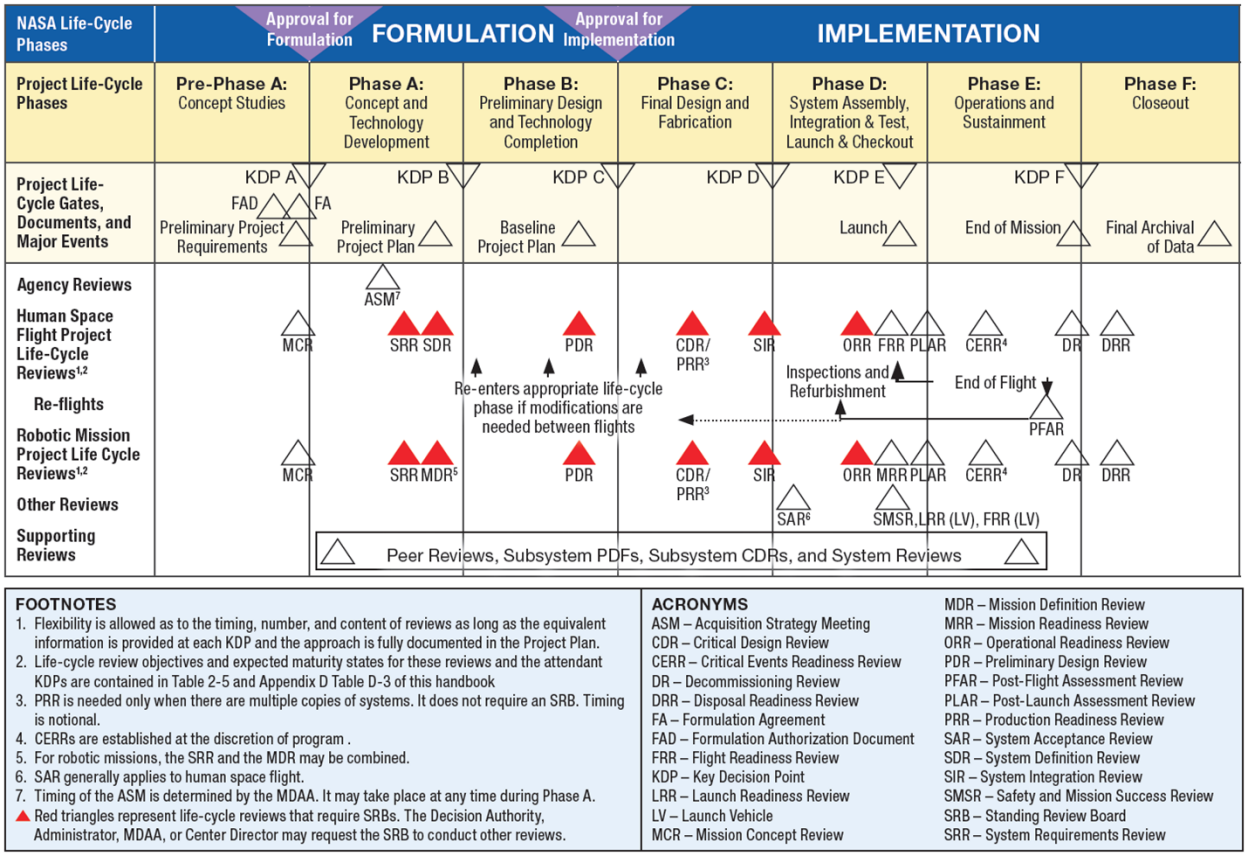


Figure 5-1. NASA's Systems Engineering Engine (Shishko 2007)

Following the well-defined NASA systems engineering handbook approach to system engineering of SoS, a well-defined review campaign will greatly improve the planning and execution of the system development.



FOOTNOTES

1. Flexibility is allowed as to the timing, number, and content of reviews as long as the equivalent information is provided at each KDP and the approach is fully documented in the Project Plan.
2. Life-cycle review objectives and expected maturity states for these reviews and the attendant KDPs are contained in Table 2-5 and Appendix D Table D-3 of this handbook
3. PRR is needed only when there are multiple copies of systems. It does not require an SRB. Timing is notional.
4. CERRs are established at the discretion of program .
5. For robotic missions, the SRR and the MDR may be combined.
6. SAR generally applies to human space flight.
7. Timing of the ASM is determined by the MDAA. It may take place at any time during Phase A.

▲ Red triangles represent life-cycle reviews that require SRBs. The Decision Authority, Administrator, MDAA, or Center Director may request the SRB to conduct other reviews.

ACRONYMS

ASM – Acquisition Strategy Meeting
CDR – Critical Design Review
CERR – Critical Events Readiness Review
DR – Decommissioning Review
DRR – Disposal Readiness Review
FA – Formulation Agreement
FAD – Formulation Authorization Document
FRR – Flight Readiness Review
KDP – Key Decision Point
LRR – Launch Readiness Review
LV – Launch Vehicle
MCR – Mission Concept Review
MDR – Mission Definition Review
MRR – Mission Readiness Review
ORR – Operational Readiness Review
PDR – Preliminary Design Review
PFAR – Post-Flight Assessment Review
PLAR – Post-Launch Assessment Review
PRR – Production Readiness Review
SAR – System Acceptance Review
SDR – System Definition Review
SIR – System Integration Review
SMSR – Safety and Mission Success Review
SRB – Standing Review Board
SRR – System Requirements Review

Figure 5-2. NASA Space Flight Project Life Cycle (Shishko 2007)

Figure 5-2 shows all of the reviews expected for complex SoS including human space flight and robotic mission projects. If strategic, these reviews can be paired down to still remain highly affective as suggested by the NASA Systems Engineering Handbook. The suggested necessary reviews are designated by solid red triangles. These reviews in time sequential order include the System Requirements Review (SRR), System Definition Review (SDR), Preliminary Design Review (PDR), Critical Design Review (CDR), System Integration Review (SIR), and an Operational Readiness Review (ORR). With implementation of this approach, future development in SoS will have a high likelihood of success due to the additional rigor needed to move from one phase of the project to the next. It will also allow the team to lock down certain aspects of the design to maximize the team's output by not allowing requirements to change after product has been flowed up as represented in the Systems Engineering Engine (Shishko 2007). For further information on the necessary inputs and outputs of each review, see NASA's Systems Engineering Handbook (Shishko 2007).

Following subsections define additional areas of lessons learned.

5.1. Team Creation, Development, and Coordination

Though the project plan did have a basic charter, there is a lack of information and responsibilities on the charter including who owns certain aspects of the project and their roles and responsibilities. At times, the lack of a clear charter made it difficult to determine who owned specific requirements and the lag in execution on requirements. This also exacerbated any direction on formal decision making that needed to be performed by an executive decision team.

The project plan also lacked a clear communication plan. This made coordination challenging at times which welcomed misinterpretation of communication frequencies, purpose, and responsibilities for each stakeholder.

In future projects of this scale, a clear project charter and communications plan will make the communication responsibilities and roles for each stakeholder substantially clearer.

5.2. Project Conception and Requirements Development

Though there are requirements and objectives defined for both CNL and Sandia, the requirements were disjointed, and there was not a single document outlining all the requirements. An attempt was made to map the requirements in a single document, but it was incomplete. The lack of a single requirements document implies the requirements development for each stakeholder was disjointed and lacked cohesion in the beginning of the project development. The observation of the lack in requirements in the observers' space and the requirements of the exercise itself also implies the lack of requirements development early in the project planning phases.

The project benefited from the automation and development of the ETE and ECS. The ETE, in particular, discovered previously undisclosed vulnerability in the HGU that simplified the exercise scenario. The design (including requirements), development, and operation of the ETE and ECS exceeded expectations.

In future projects of this scale, a clear requirements development period will substantially simplify validation and verification that the project is fulfilling the customer's and stakeholder's requirements at the end of the project. The formal execution of an SRR and SDR will allow all stakeholders an opportunity to provide concurrence on defined requirements and the overall system design. These reviews also force a formal review board to review and approve any additional requirements not already approved.

5.3. Planning

Due to the lack of clear requirements definition and sign-off in the beginning of the project, definitions and expectations of testing events became misaligned when the events were being planned and executed. Another causal event that misaligned expectations of planning and execution of testing events was the lacking charter. With a clearer charter, stakeholders would have had clear direction on the roles and responsibilities of each stakeholder at the events. It would not have cleared up every misaligned expectation, but it would have simplified discussions on if items requested were within scope or out of scope.

In future projects of this scale, clear requirements and roles and responsibilities will simplify the planning of the testing events required for an event of this size.

5.4. Execution

Along with the lack of overall project requirements, there was a lack of reviews on the progress of the evaluation methodology being developed and the project itself. There were several reoccurring project meetings, but the intention and expected outcomes could have been better defined. This lack in review lead to the addition of objectives and requirements very late in the process that needed heroic acts by team members to complete on time.

In future projects of this scale, a clear testing campaign will allow the team to better plan and prepare for the full-scale exercise. An adaptation of the well derived NASA Systems Engineering Handbook timeline (Shishko 2007) will provide a structure to enable necessary reviews during the development and execution phase of the project to minimize stakeholder misalignment.

5.5. Artifacts

The number of stakeholders from different organizations on this project made it clear that the availability of a file repository that is easily accessible by all stakeholders is necessary, albeit complicated to maintain. INL initially hosted a file repository, but the maintenance of that repository faltered going into 2023.

In future projects of this scale, a well-organized repository that is easily accessible by all stakeholders will allow the team to maintain artifacts and archive them throughout the life of the project.

The ECS development accounted for ambiguity in the overall project requirements and MSEL. However, the ECS is versatile, scalable, and flexible that can readily support many of the MSEL permutations.

REFERENCES

BSI. (2009). *BSI-Standard 100-4, Business Continuity Management.* Germany: Federal Office for Information Security (BSI).

Haapahovi, S. (2017, July 21). *Method for Dealing with Uncertainty: The OODA Loop.* Retrieved from https://medium.com/@haapahovi/method-for-dealing-with-uncertainty-the-ooda-loop-6deb2232c11e

OODA Loop. (2023). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/OODA_loop

Rowland, M. (2022). *Final Planning Meeting Canada-USA Blended Attack Exercise Experimetn Approach, SAND-2022-15027PE.* Sandia National Laboratories .

Shishko, R. (2007). *NASA Systems Engineering Handbook, Revision 2.* Washington, D.C., USA: National Aeronautics and Space Administration.

Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015, January). A Secure Control Framework for Resource-Limited Adversaries. *Automatica, 51*, 135-48.

APPENDIX A. WKID AND OODA CONCEPTS

WKID-OODA Loop concepts were used extensively for the observer experience and assisted greatly in the success of the event. A key part of WKID-OODA Loop to structure in a simplified manner the key MSEL events and assign them. The WKID Concept was introduced with the following points:

(1) Technology performs many critical functions for nuclear security
(2) These functions support key processes for physical protection and cybersecurity
(3) Technology and processes are key to provide WKID for people to make good decisions and undertake good actions.

The following figure outlays the key elements and details of each element of the WKID triangle:

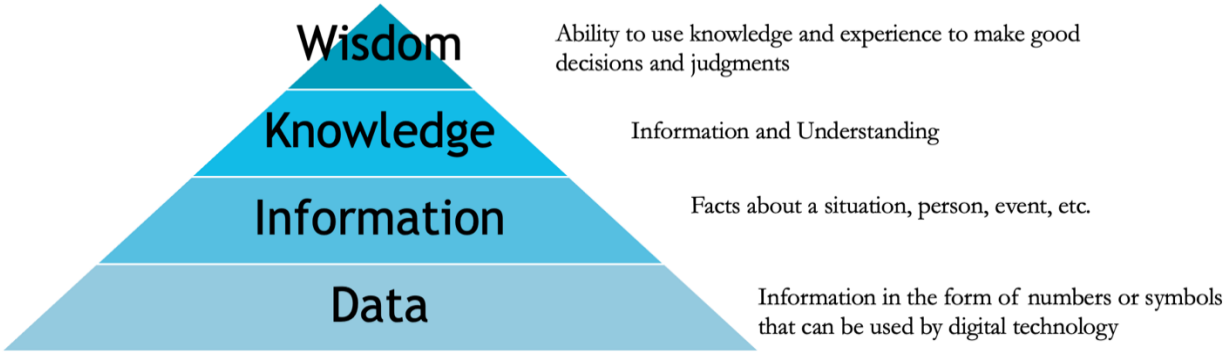


Figure A-1. WKID Triangle

The OODA Loop was introduced early in the initial planning of the exercise and described as follows (Rowland, 2022):

- Decision making process that allows for agility in making decisions in situations where information is incomplete or uncertain.
- An entity that can process this cycle quickly, observing and reacting to unfolding events more rapidly than an opponent, can thereby "get inside" the opponent's decision cycle and gain the advantage (OODA Loop, 2023).
- Entities can be individuals or organizations
- Act – requires familiarization with a target environment and organization.

As the exercise was to be hosted at Sandia's ISF, the "act" or "actions" of Bruce Power would be similar but would not match their performance of the OODA Loop at their facilities. However, there are decisions that could be captured or the intention to act that would indicate whether "wisdom" from WKID triangle has been attained. Therefore, the exercise looked to evaluate OOD:

- Observe – cyber effects and alerts should be intuitive for a minimally qualified individual or capable organization
- Orient – information should be in a form that allows for connection with the exercise/environment
- Decide – key criteria for the evaluation methodology

Figure A-2. OODA Loop (Haapahovi 2017)

Additional constraints on time duration and tempo of the exercise (compressed vs. realistic), further evaluation of performance leveraging the OODA Loop were not possible. However, relative and anecdotal evidence of correct completion of key tasks and the "sense-making" of incomplete or ambiguous data and information into knowledge and wisdom. Both concepts have as their objective the making of good decisions and undertaking of good actions.

APPENDIX B. THE CONVERGENCE OF WKID-OODA LOOP

The Cyber Book of Knowledge v.1.0 provides a notional model of a sense-making loop for analysts that can be simply adapted for the WKID-OODA concepts. The OODA loop requires performance of all activities to upgrade Data and Information to Knowledge and Wisdom. The overarching requirement is to decide and act to protect the facility from the attacker. However, since the WKID triangle is incomplete, there are potential decisions and subsequent actions can be categorized into two objectives:

1. Personnel determine that data and information is insufficient and cannot be upgraded, therefore decision to acquire or gather more data and information. This type of process is a "foraging loop".
2. Personnel are able to upgrade the data and information to knowledge or wisdom. This type of process is a "sense-making" loop.

The overall process is guided by OODA Loop, but tasks can be simplified by one of these two main objectives. The two types of subloops are expected to be concurrent and several loops of each type of loop may be concurrent dependent on the size of the exercise. A simplified figure showing the WKID-OODA notional model with a single foraging and sense-making loop and foraging loop is shown below.

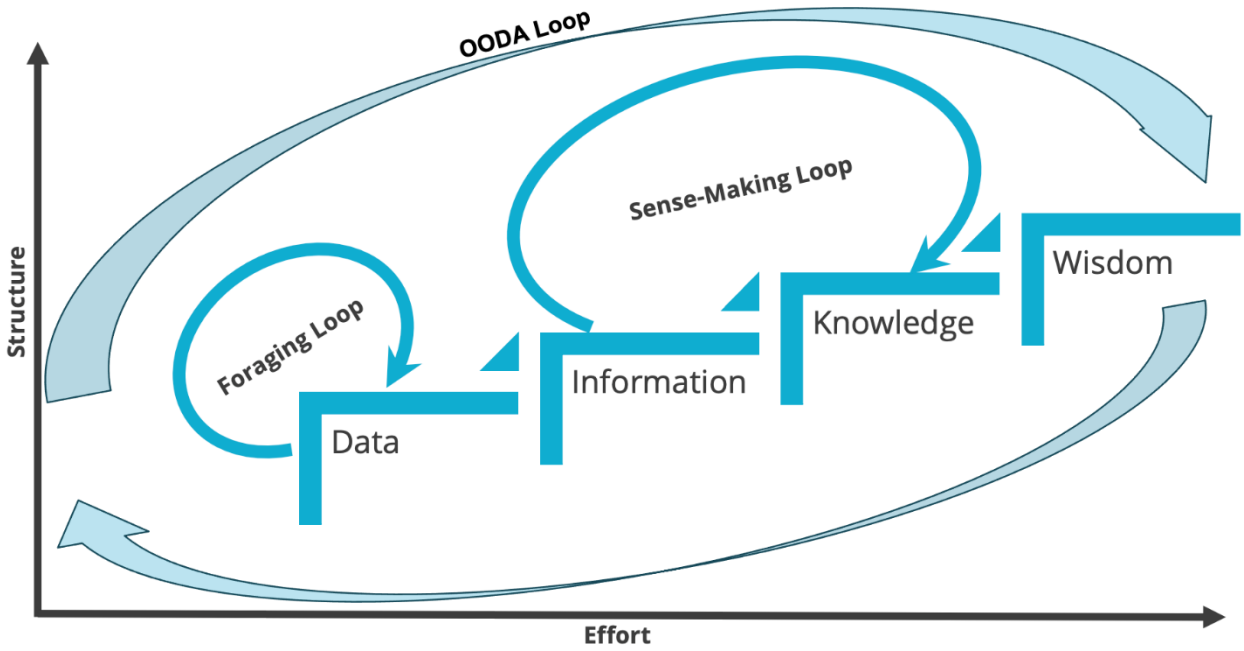


Figure B-3. Notional Model of WKID-OODA Concepts

The notional model provides some indication of the structure and effort to achieve the functional requirements as outlined in WKID. However, each of the loops may vary in the structure and effort and do not strictly apply to the indications. The key is that foraging loops, generally apply to Data and information and are fully performed within one or both levels. Foraging loops require technology to gather data and is supported by people and processes. Information can be gathered from any source. For example, foraging loops could be near real time (i.e., almost immediate) where mature technology (like a Cyber SOC) automatically gathers and displays the data. A typical instance

would be for a Cyber SOC analyst to run a pre-developed script to generate a web page displaying the information as data, or in the case of the scenario the Cyber SOC analyst would need to call the RSE to discuss with the vendor as to a possible cause of the alert, or open bulk and unstructured raw network logs and start to identify critical information for subsequent sense-making loop. The pre-developed script would take much less effort and time compared to the other two options.

The Sense-Making Loop is performed to upgrade the lower levels to the upper tiers. This occurs when a decision point is reached, like calling an incident, where personnel meet and discuss the available information. In the case of the exercise, the RSE provided information that the vendor was aware of the type of error on the HGU and was investigating the matter. Sense-Making loops take tremendous effort when the event is previously unencountered or unknown, requiring analysis to be completed "on-the-fly".

Both foraging loops and sense-making loops impact time and resources. However, in the case of the exercise, the WKID-OODA loop does provide some insights that may be applied to reduce challenges with meeting performance requirements in the future.

APPENDIX C. PEOPLE, PROCESS, AND TECHNOLOGY

People, process and technology are key contributors to a successful and well managed Nuclear Security program. However, cybersecurity is a relatively new concern for Nuclear Security and guidance on concepts that can inform investments in these resources is incomplete.

During the observer experience, the WKID triangle was presented that aligned these contributors to their potential capabilities. The table below summarizes the discussion:

Table C-1. WKID Triangle Discussion

Contributor	Applicable WKID Objects	Rationale
Process	All Levels	There are many processes that impact incident response: (1) Playbooks, Complex Troubleshooting Plan/Guide (2) Technology design and customization, this includes time spent to pre-develop scripts and analyst views (3) System design and testing – baseline of system behavior can provide valuable information (4) Training and Security Culture, Policies – training can minimize time to gather further information, policies and security culture can support good decisions on incomplete information.
People	WKI	People cannot read or capture "data"; all data is displayed in human readable form after it has been read by the technology
Technology	KID	Technology can be developed via processes to gather extensive data, upgrade to information, and potentially knowledge, especially for cyber-attacks that are previously known (i.e., knowledge-based detection; e.g., malware/anti-virus program).

APPENDIX D. WKID BINGO CARD

The following table was developed for the exercise and provided to the participants and provides support for the predictive value of WKID.

Table D-2. WKID Bingo Card – Filled Out

Event #	EVENT DESCRIPTION	DATA	INFO	KNOWLEDGE	WISDOM
1	**HGU Manufacturer: Bad Checksum Behavior has been reported and an investigation is ongoing.**		People & Process		
2	**Responsible System Engineer (RSE): Manufacturer report indicates loss of access control configuration**			People & Process	
3	**CSOC/SIEM: Configure an alert for HGU Bad Checksum**	Technology & Process			
4	**Cyber Security Operation Centre (CSOC)/Security Information Event Management (SIEM): Unusual Account Login**	Technology			
5	**CSOC/SIEM: Powershell Command Executed**	Technology			
6	CSOC/SIEM: Bad Checksum on Hand Geometry Unit (HGU)	Technology			
7	**HGU: Removed Entry from User Access List**	Technology			

Event #	EVENT DESCRIPTION	DATA	INFO	KNOWLEDGE	WISDOM
8	**CSOC/SIEM Alert: Bad Checksum Alert on HGU**		Technology & People		
9	**HGU: False Negative for single user**		Technology & People & Process		
10	**HGU: Contractor access restored by Adversary**	Technology			
11	**HGU: Adversary access is added**	Technology			
12	**CSOC/SIEM: Additional Bad Checksum Alerts**		Technology & People		
13	**RSE: Gather more information on HGU Access Control Logs (Foraging Loop)**		People & Process		
14	**CSOC Operator/CAS Operator: RSE provides understanding of impact of Bad Checksum Alert on the Access Control Logs**			People & Process	
15	**CSOC Operator/CAS Operator/RSE: Decision to initiate incident response**				People & Process

Events provided by default to the CSOC team during the MSEL:

- #3 - CSOC/SIEM: Configure an alert for HGU Bad Checksum; provided to ensure Bruce Power would not require to undertake Threat Hunting activities.
- #6 and #8 - CSOC/SIEM Alert: Bad Checksum on Hand Geometry Unit (HGU); 2 Alerts

These alerts would prompt CSOC analysts to reach out to the RSE for further information, knowledge and wisdom to determine whether the alerts were known to be associated with a potential attack. The first response from the RSE was based on Events #1 and #2, which did not provide any knowledge or understanding of the potential cause of the alert.

The RSE also informed the physical protection staff that there was a CSOC alert on the HGU. The CSOC team had several discussions as to whether this was an attack or some typical malfunction. Particularly confusing was the wording of the alert "Unusual Account Login". Focusing on the alert from the CSOC rather than Event#2. These discussions repeatedly mentioned "Unusual Account Login" and this vocabulary delayed calling an event.

Conversely, at the same time the Physical Protection staff focused on Event#2 and immediately commenced their preparations for an incident response and management despite not receiving the initial notification of the cyber event.

D.1. The Role of Security Culture

WKID concept applied retroactively to the exercise would indicate that both teams did not know the cause of the events or its potential impact to the site. However, the physical protection staff demonstrated that they escalated and engaged much faster than the CSOC team as their main objective was to ensure security which was called into question by the CSOC alerts and Event#2. Discussions afterword indicated that the physical protection staff is continually trained to understand and believe that the threat is real and adversaries are targeting the facility, the key beliefs of security culture, and have a questioning attitude and conservative decision making. The difference in vocabulary was significant with the CSOC using the alert language "unusual account login" where the physical protection team used "potential unauthorized access to the protected area".

Physical Protection staff in the hot wash indicated they have the resources to respond and sustain the heightened security measures for a longer duration with an extra shift of personnel to provide on-demand qualified resources. Cyber Security staff indicated they only have enough staff for a Monday to Friday 9am to 5pm monitoring with no additional staff that could be directly leveraged to support. Additionally, CSOC staff indicated that the impact of initiating a prior event impacted staff and leadership, resulting in increased hesitancy to call an event.

The role of strong security culture provides:

1. Qualified and immediately available staff necessary for incident response
2. Protection from criticism or impact on job evaluation for making conservative decisions
3. Reduction in the data, information, and knowledge demands necessary for making these conservative decisions.

Given the scenario duration, an event lasting 4-5 hours could easily be sustained. However, cyber attacks may occur over months which has the potential to raise costs to an unacceptable level. This scenario provides insights into what enables faster responses, but did not consider these faster responses to "false alarms" or the costs to sustain over a longer period.

The result was the CSOC staff needed greater certainty to initiate an event. The initiation of the event was approximately 75 minutes after that of the physical protection staff.

D.2. Predictive Power

While the CSOC team was engaging in discussions, they actioned the RSE to gather the logs on the HGU. This request aligns strongly with the foraging loop, as the data and information was too incomplete and ambiguous to initiate an event. During this time, the CSOC team was actively trying to complete the sense-making loop, but lacked clear and direct information to provide them with the knowledge to undertake a decision.

Unfortunately, it was clear that the CSOC team would not complete the sense making loop without additional information which was provided which were:

- Event #7 - HGU: False Negative for single user
- Event #9 - HGU: Contractor access restored by Adversary
- Event #10 - HGU: Adversary access is added

While the events were detailed as the Adversary action to align with the MSEL, the report from the RSE just indicated additions and deletions of the users and not indicated it was an actual attack. Unfortunately, due to timing constraints and a pre-scheduled break, Event#13 providing the knowledge of the data and information that was needed to make a decision. It would be interesting to perform the scenario where increased time was available to determine the performance and hopefully successful completion of a sense-making loop.

During the observer experience, the WKID table above was provided and used to predict the necessary data and information that was needed for the CSOC team to initiate an event. The threshold of evidence both in its certainty and structure was much higher for the CSOC team and this certainty is captured in the WKID table of events. It was repeatedly stated that the CSOC team would not call an event unless certain it was an attack. With the initial events, it would have been impossible to be certain that the cause was an attack.

Additionally, once the impact was clear and understood Event#13, the prediction of WKID events table would be the event would be almost immediately initiated, which in fact, it was. The time between Event#13 and #14 was approximately 30 minutes.