FERC Security Program for Hydropower Projects

Frequently Asked Questions

1. **Question:** My dam and powerhouse utilize the same network, is it accurate to consider those two physical locations as one cyber asset?
Answer: *Yes, but you must consider 1. the consequence parameter which determines criticality would come from the higher of the two assets, and 2. for any physical protection measures (e.g. baseline item #1) they must be applied at both locations.*

2. **Question:** My dam and powerhouse are on separate satellite links so is it safe to assume that each would be evaluated independently for consequences?
Answer: *Yes, provided there is no exchange of information between the two networks.*

3. **Question:** Can you provide clarification on "full or partial loss of reservoir"?
Answer: *Yes, the reservoir could be lost entirely if for example, spillway gates remained closed which lead to an embankment overtopping and releasing the entire reservoir. Another example is if a powerhouse bypass was opened and the reservoir drained to the intake invert. In terms of partial release, spillway gates could be opened and the pool above the spillway sill would be lost.*

4. **Question:** Can mitigating measures be used to <u>not</u> classify my asset as "operational"? For example, my operator visits the dam/powerhouse on weekends and would notice if spillway gates or a low level outlet were releasing the pool. Also, I have telemetry that tells me if something is going wrong.
Answer: *Mitigating measures can <u>only</u> be used to prevent an asset from being classified as critical. For example, opening a spillway gate or powerhouse bypass has the potential to at very least create an initial uncontrolled surge of water which could create a threatening condition downstream. Telemetry can only be relied on (similar to independent stream gages) if it's on a separate network[1] than that of the cyber asset under evaluation and the telemetry can be verified as trusted.*

5. **Question:** Only my wicket gates can be compromised at the powerhouse to release flows and my operator would see that on a site visit. Does my little bit of flow as compared to channel capacity, require me to consider my cyber asset as at least operational?
Answer: *Several factors should be considered in addressing this question as each site is different. Consideration should be given to whether there is recreation in the tailwater's immediate vicinity that could be impacted by a surge of flow, if a dam downstream could be overtopped during a sustained release, if an upstream dam could become unstable*

[1] A separate network is defined as a network that has no ability to communicate with another network required to be compliant.

because of the lowered reservoir, or if wicket gates can be quickly closed causing harm to the generating units and other water hammer induced implications. If any of these are possible, then the asset should be considered operational. When in doubt, deference to classifying the asset as operational is preferred because even if consequences appear to be none, good cyber security practice dictates that only authorized users be able to gain access to control systems. The thought process of this should be well documented to support the decision. In terms of estimating volume of flow possibly released to determine whether the asset rises to the level of critical, 48hrs is a good starting point. Even if the asset is not determined to be an operational cyber asset, from a cyber perspective it is a best practice to evaluate network connectivity to ensure if the wicket gate controller is compromised there can be no malicious movement into other controllers or network segments.

6. **Question:** If our full generation flows were started and went undetected, the lake could drop below the intake pumps for city water supply. However, we have contractual control of the upstream dam and could quickly call for a water release that would restore water at their intake. Is this sufficient to require baseline only or must we do the enhanced?
Answer: *Baseline measures would be required, but to determine if enhanced measures would apply, you would have to evaluate reservoir volume lost until detection and coordination could happen and compare that to a reliable inflow to be released into the reservoir. If detection and upstream response time could allow for water levels to drop below the intake, enhanced measures should be applied unless other means for detection and response are implemented. This is similar in the sense that dependent upstream features need to be considered when scrutinizing a compromised asset. For example, loss of the reservoir could cause rapid drawdown failure of embankment slopes well above the full pool being lost or intake pumps of a nuclear powerplant's cooling system could be lost. From a cyber perspective, interconnectivity, communication and control of the upstream dam should be considered even if not under FERC jurisdiction because the compromised generation networks of the FERC jurisdictional asset could have impacts on the upstream dam and its ability to carry out the necessary releases.*

7. **Question:** My powerhouse only generates 500kW and if compromised, wouldn't really cause any impacts, but would be an operational cyber asset following the Cyber Asset Designation Flowchart on page 38 of Revision 3A. This doesn't seem to meet the intent of the Guidelines, can you clarify?
Answer: *Although it is good cyber security practice to protect all cyber assets, we acknowledge there should be a threshold on "Losing power generation." Therefore, we have incorporated into Table 9.1c two threshold values to establish if it's a critical or operational cyber asset. In addition, if installed capacity or total capacity controlled by one cyber asset is less than 100 MW, it is considered non-critical. Furthermore, if a*

generating unit qualifies as having black start capability, it is considered an operational cyber asset.

8. **Question:** Our dams are not remote operated, does this make us exempt from the requirements?
Answer: *No, applicability to Section 9 only applies for the year and must be reassessed annually or when there is a change to remote capability. In addition one should always establish policies and procedures for the use of removable media in order to prevent the infection of non-remote systems, which may be the source for future infections and/or the installation of a logic bomb.*

9. **Question:** Our remote operating networks are air gapped. There is no external connection and the link from the dam to the remote control room is a dedicated fiber optic line. For the intent of Table 9.1a, would we select "no" for remote operation?
Answer: *Yes, that is correct. However, good cyber security practice dictates that physical and cyber protection measures should be placed on that equipment to protect unauthorized access such as locked doors with keycard access and implementing security policies for removable media (i.e., USBs), respectively.*

10. **Question:** Can you explain air gapped, automated, segmented, and interconnected?
Answer: *<u>Air gapped</u> system is when there is a logical and physical isolated system/network with no communication capability to any other system by any means. The air gapped system is essentially an isolated island with the only means for access is the physical presence of on operator on the system and the use of mobile media to move files/updates in and out of the system. If an operator can access the system without physically being present it is not considered an air gapped system.*

<u>Automated</u> is when an action is initiated because a processing rule is matched. The automated response can be triggered when a detected condition, such as an event, an alert, a performance sample, or a performance threshold is matched. For example, in a programmable logic controller (PLC) logic could be written so that when the reservoir elevation reaches a specified level, spillway gates (or low level outlet) open.

<u>Segmentation</u> is when two or more networks with different trust/functionality are physically and/or logically protected from each other (i.e., router, virtual local area network – VLAN). These segmented networks may or may not need to communicate with each other; therefore, security controls are implemented between the segments to assure only permitted network communication can be exchanged between the segments (permitted communication may be none).

<u>Interconnected</u> for the purposes of the Guidance document is when a cyber asset (e.g. control center) has the ability to exchange information, via a connected network, between Security Group 1&2 dams and Group 3 dams. The intent here is to insure that no "weakest link" exists at the Security Group 3 dam.

11. **Question:** In terms of cost for my situation, it’s cheaper to turn my cyber asset into an air gapped system or local controlled system. Is there anything preventing me from doing this?
Answer: *With respect to Section 9 there is not. However you must fully evaluate whether the action would cause any dam safety or emergency action plan implications. For example, you don’t want to reduce your response time to open gates to pass a large flood.*

12. **Question:** I have a spoke and hub system and my hub falls under both Section 9 and under NERC-CIP**,** what do you expect from me?
Answer: *With respect to the hub, you must provide a reference in your Security Plan as much and provide the inspecting engineer all NERC documentation related to that asset for review, which should include items such as results of a NERC compliance audit or internal review and recommendations. As for the spokes, each of these should be evaluated with respect to Section 9 with close attention paid to any interconnection with Security Group 3 dams.*