Identification of Critical Digital Assets

ANDREW MEYER, SAFETY ANALYSIS MANAGER

Critical Digital Assets (CDA)

- SHINE Technologies identifies and protects digital assets that, if compromised by a cyber attack, would cause a consequence of concern.
- Not all digital assets require protection.
- SHINE's approach determines which digital assets require cyber security controls, can be protected by alternate means.

Critical Digital Assets (CDA), Step 1

- Step 1: Identify digital assets associated with consequences of concern
  - Consequence of concerns are defined as:
    - Latent – Safeguards: The compromise, as a result of a cyber-attack, of a function required to prevent unauthorized removal of special nuclear material (SNM) of moderate strategic significance.
    - Active – Safety: Exceeding the SHINE Safety Criteria as a direct result of a cyber-attack.
    - Latent – Safety: The compromise, as a result of a cyber-attack, of a function required to prevent or mitigate the consequences of an accident which could exceed the SHINE Safety Criteria.

Critical Digital Assets (CDA), Step 1

	SHINE Safety Criteria
a[1, 2]	An acute facility staff dose of 5 rem or greater total effective dose equivalent (TEDE)
b[1, 3]	An acute dose of 1 rem or greater TEDE to any individual located outside the owner controlled area
c	An intake of 30 mg or greater of uranium in soluble form by any individual located outside the owner controlled area
d[1, 4]	An acute chemical exposure to an individual from licensed material or hazardous chemicals produced from licensed material that could lead to irreversible or other serious, long-lasting health effects to the facility staff or could cause mild transient health effects to any individual located outside the owner controlled area
e	Criticality where fissionable material is used, handled, or stored (with the exception of the target solution vessel)
f	Loss of capability to reach safe shutdown conditions

[1]Acute refers to a single radiation dose or chemical exposure event.

[2]The control room operator dose is evaluated over a 30 day period, except for accident scenarios involving the tritium purification system, which assumes a 10-day exposure event. The RCA worker dose is evaluated for a 10-minute evacuation period for evacuation.

[3]The public exposure event is generally assumed to last for 30 days for all events, except for accident scenarios involving the tritium purification system, which assumes a 10 day exposure event.

[4]Hazardous chemicals produced from licensed material are substances having licensed material as precursor compound(s) or substances that physically or chemically interact with licensed materials, or are comingled with licensed materials.

Critical Digital Assets (CDA), Step 1

- Identify site areas and processes associated with a consequence of concern.
  - Examine areas and processes for:
    - functions that could be compromised to directly cause a safety consequence of concern (i.e., active)
    - functions needed to prevent a consequence of concern (i.e., latent)
  - Examine those functions and identify the role of digital assets.
  - Determine which of types of consequences of concern potentially apply if a compromise of the digital asset were to occur.
  - Determine whether the compromise of the digital asset would lead to a consequence of concern if a secondary event occurred (i.e., SHINE Safety Analysis considered initiating event). To make these determinations, review:
    - software platforms and applications related to digital asset functions or processes
    - communication and data flow involving the digital asset

Critical Digital Assets (CDA), Step 2

- Step 2: Determine CDAs by considering alternate means.
  - Consider the function of the digital asset to determine whether an alternate means exists that could be credited or implemented to prevent the consequence of concern.
    - The availability and usage of an alternate means is an equivalent substitute for the function provided by the digital asset in lieu of protecting the digital asset via cyber security control.
  - When considering acceptable alternate means, SHINE considers attributes, such as:
    - are protected from a cyber attack
    - are sufficiently reliable and adequately implemented consistent with other safety or security features
    - are properly maintained and periodically tested
    - prevent the identified consequence of concern
    - can be activated in a timely manner to prevent the identified consequence of concern
    - would be implemented with available resources
    - do not contribute to other vulnerabilities or lead to a consequence of concern

SHINE

Critical Digital Assets (CDA), Step 2

- Crediting a manual action as an acceptable alternate means should only be done after determining that the action is reliable.
  - The compromise of a function by a cyber attack is extremely difficult to detect and should not be relied upon to initiate a manual action (i.e., reactive actions are generally not acceptable alternate means).
- If no alternate means exist for a digital asset, it is a CDA.

Critical Digital Assets (CDA) Documentation

- Final results of CDA analysis are documented in a technical report, including the following information:

Name	Location	Consequence of Concern	Alternate Means Present (yes or no)	Description of Alternate Means (if applicable)	Implementing Control (applicable for CDAs)
Digital Asset		Active - Safety Latent - Safety Latent-Safeguard			