For high and medium impact BES Cyber Systems with a defined ESP, classification of network devices is less of an issue because such devices are clearly either (i) out of scope or (ii) identified as a BCA , or (iii) identified as PCA, which receive a commensurate level of protection as a BCA.

In general, network devices do not perform application logic of the reliability function, but certain network devices may be a necessary component in the workings of the BES Cyber System. This Lesson Learned presents approaches used by Implementation Study[1] participants to categorize network devices associated with high and medium impact BES Cyber Systems.

Guidance

Examples of the approaches taken by study participants are described below. The classification of communication and networking devices is described as well as several diagrams to show some examples of the approaches taken.

Network Devices Classified as BES Cyber Assets

As the study participants evaluated the reliability tasks performed at each asset, participants recognized that certain network and communication devices should be categorized as BES Cyber Assets. The determination was based on the assessment that if the network devices were rendered unavailable, degraded or misued they would have the potential to adversely impact the reliable operation of the asset. One example was a network device providing backbone communication for the local BES Cyber System. Another example of this network device might be a core switch passing traffic between devices on a plant control network or substation network. In contrast, the communication and networking devices that were only being used for external communications did not have an impact on the reliability tasks performed at the asset and, in turn, were not classified as BES Cyber Assets.

Network Devices Classifed as Protected Cyber Assets

The study participants also recognized that certain network devices, while not identified as a BES Cyber Asset, would meet the definition of a Protected Cyber Asset (PCA). Specifically, network devices may reside on the same local, routably connected networks as BES Cyber Systems but would not meet the definition of a BES Cyber Asset because if the network device were rendered unavailable, degraded or misused, it would not have the potential to adversely impact the asset. For example, a network device might be a network switch added to create a way to gather all the event data from multiple devices into a single device for analysis at a future time. Because the network devices have a routable connection to a BES Cyber System and was included inside the ESP by the participants, the network device was categorized as a Protected Cyber Asset associated with the medium impact BES Cyber System.

Examples

[1] Ref. Implementation Study Final Report http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf