NERC Cyber Security Standards: Risk Based Methodology

May, 2009

Background

NERC CIP-002 R1.2 requires Responsible Entities to identify their critical assets using a risk-based methodology. Risk-based methodologies usually consider the threat (likelihood) of an event and its consequences. The IESO[1] recognizes that cyber attacks will happen; therefore our risk-based methodology focuses on the mitigation of consequences.

Critical assets are those which, if destroyed, degraded or otherwise made unavailable, would affect the reliability or operability of the Bulk Electric System. In the context of cyber security, a denial of service attack makes the asset unavailable. A loss of control and/or monitoring of critical assets would have a significant impact on reliability, including our ability to restore after a partial or total blackout. However, we must also protect these assets from unauthorized operation. Multiple element contingencies without accompanying faults are very probable for a scenario where a malicious party takes control of a critical asset such as a transmission substation.

In Ontario, the criteria used in determining critical assets address the traditional 'impact on the interconnection' for asset loss, but also consider our ability to restore after a blackout as essential in maintaining an adequate level of reliability and mitigating the impact on public health and safety.

The criteria were developed in consultation with Ontario's Emergency Preparedness Task Force, which includes key market participants and government representatives. It includes a cross-reference to the requirements of NERC CIP-002, which describe the types of assets that must be considered.

In developing the criteria, we considered:

- The list of bulk power system elements derived using NPCC A-10 *Criteria for Classification of Bulk Power System Elements,*
- An additional assessment using the non-fault based extreme contingencies as listed in NPCC A-2 *Basic Criteria for the Design and Operation of Interconnected Power Systems*¸ which recognizes the credible nature of total station loss, SPS false operation or SPS failure to operate under a cyber attack scenario
- Elements that form the basic minimum power system as defined in NPCC Directory 8 *System Restoration* and identified in the Ontario Power System Restoration Plan (OPSRP)

[1] In this document 'we' and 'our' means IESO

- Based on experience during the 2003 blackout, any additional elements, including generation, that we require to effectively implement the restoration plan
- Control centres that perform monitoring, control or configuration of any critical assets

Criteria

In order to apply the NERC cyber security standard definition of critical assets in Ontario, the following criteria identify the power system assets needed to restore and reliably operate the IESO-controlled grid. These assets are necessary to mitigate the impact of a prolonged power outage on Ontario's public health and safety and achieve three basic principles.

- Enable the reliable operation of the bulk electric system.
- Restore the grid from blackout conditions to the point where the grid can be energized and is reasonably stable. This requires about 11,000 MW of load and generation, which is less than half Ontario's demand, but is sufficient to enable restart of other generators to supply the remaining load.
- Protect critical assets whose loss could result in an unacceptable impact on reliability (e.g. cause a step-change to tie line flows which would likely adversely affect Ontario's interconnected neighbours)

#	Criteria	NERC CIP-002 Reference

1.	**Transmission**
	• Transmission stations on a restoration path[2] (as described in the Ontario Power System Restoration Plan). Includes transmission stations:
	  ○ In series with the preferred restoration path
	  ○ Needed to synchronize restoration paths to create a larger electrical island
	  ○ To significant interconnections (Michigan, New York, Quebec-Beauharnois)
		R1.2.2

	• Transmission stations whose loss could have significant adverse impact on the interconnection (i.e. those identified as Bulk Power System elements using NPCC A-10)	R1.2.2
	• Generating station switchyards in series with or required to initiate a restoration path	R1.2.4

[2] "Restoration path" is equivalent to the NERC-defined "cranking path" (ref. NERC Glossary of Terms)

#	Criteria	NERC CIP-002 Reference
2.	**Generation** • Generating stations, nominally[3] > 300 MW • Generating stations under contract with the IESO to provide blackstart • Generating stations under contract with the IESO to provide significant AGC Note: Assets regulated by the Canadian Nuclear Safety Commission are exempt from NERC CIP-002. However, owners/operators of such facilities are encouraged to adopt these standards.	R1.2.3 R1.2.4 R1.2.3
3.	**Operability** • Control centers that: o Control generation > 300 MW (aggregate) o Operate equipment falling under criteria 1 or 2 o Fulfill Reliability Coordinator functions (i.e. the IESO) • Facilities that concentrate the data from three or more control sites that are required to monitor, operate and protect power system equipment falling under these criteria • NPCC Type 1 Special Protection Systems	R1.2.1, R1.2.5, R1.2.6 R1.2.4, R1.2.7 R1.2.6

[3] Threshold used as a trigger to consider the asset, not an absolute value. Other considerations include the importance of the generator for voltage support, proximity to a restoration path, and relative impact on bulk power system reliability.