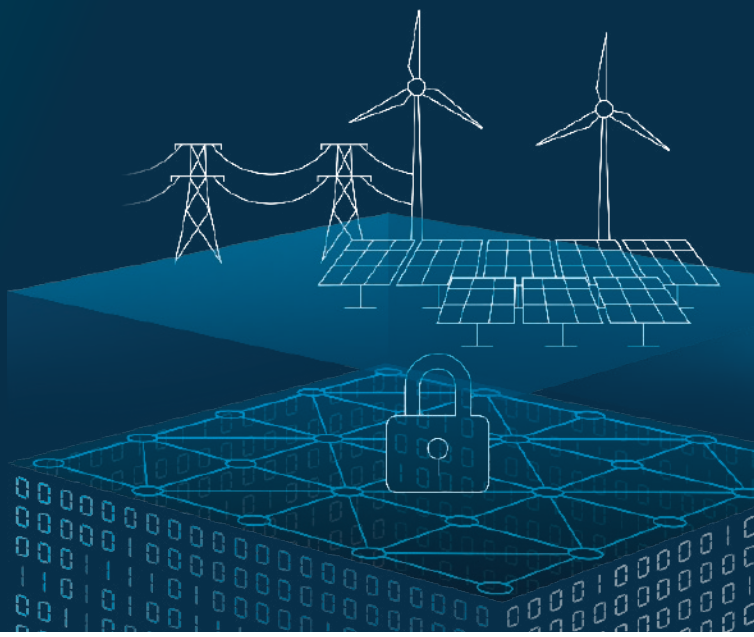
SNC·LAVALIN
Building what matters

Security maturity assessment program (SMAP)

Securing what matters



Critical infrastructure protection is a top priority for utilities as the power sector faces increasing network interconnectivity, widespread smart grid technology and ever-growing cyber and physical threats. We understand the challenges utilities face on their journey to secure their infrastructure and comply with regulatory requirements. To facilitate that journey, SNC-Lavalin developed a program tailored for power utilities to measure the maturity level of their physical, cyber IT/OT and human resources security programs.

Security maturity assessment tool

The first step of our assessment consists of using our in-house tool. One of its key feature is its ability to automatically generate a report that allows clients to quickly measure the maturity level of their physical, information technology, operational technology and personnel security programs against leading industry security standards.

20 security domains across 3 streams

IT/OT SECURITY

> IT/OT governance
> Risk management
> Asset management
> Identity and access management
> Data security
> Host security
> Network security
> Situational awareness
> Incident response
> Operation integrity

PHYSICAL SECURITY

> Physical security governance
> Perimeter barrier
> Security lighting
> Video surveillance
> Intrusion detection
> Physical access
> Security locks and keys

PERSONNEL SECURITY

> Background checks
> Security awareness
> Security training

Security standards

The latest and most stringent industry security standards are used:

> NERC – Critical infrastructure protection standard
> NIST 800-53 – Cybersecurity framework
> NEST 800-82 – Industrial control systems security
> ISO 27001 – Information security management
> IEEE 692 – Security systems for nuclear power generating stations

Workshops

A proven methodology is used to perform the assessments, whereby the SNC-Lavalin team leads a dedicated workshop for each security stream. The participation of key power utility stakeholders possessing a thorough understanding of the operations is imperative. During the workshops, the applicable security controls generated by our tool are discussed and our experts populate it with the pertinent information collected.

Required documentation

Prior to hosting the workshops, you will be required to provide copies of your security policies, IT/OT/Security organizational charts, network security architecture, incident response procedures, disaster recovery procedures, penetration test reports, security auditors' reports, etc. This information allows our team to better understand your security program and results in a more effective interaction and output during the workshops.

Final assessment report

Our tool generates a separate report for each security stream (i.e. IT, OT, physical security and personnel security). The reports provide an evaluation of up to 300 security controls, along with detailed recommendations and a suggested roadmap on the most cost effective approach to mitigate them.

Speak to our experts

cip-ot-digital@snclavalin.com

snclavalin.com/en/inc