Critical Infrastructure and Control Systems : How to protect?

Sabbir Hossain

Cell interception system, Cell interrogation & active tracking system, critical infrastructure security, tactical & intelligence solutions

There are many ways to define "Critical Infrastructure," but what these definitions have in common is most closely conceived of as infrastructure that would affect the economic and national security of a country if it were negatively impacted or eliminated. The U.S. Department of Homeland Security describes critical infrastructure as the resources, structures, and networks, either physical or electronic, so important to the U.S. that their loss or failure will impair security, national economic defense, national public health or safety, or any combination thereof. The EU, as well as several other sovereign countries, often recognize as part of critical infrastructure numerous measurable and internet-governed elements.A layered approach is needed to secure critical infrastructure against growing and evolving cyber threats. Governments should work actively with public and private partners on a daily basis to prevent, respond to and coordinate efforts to mitigate attempted disruptions and adverse impacts on the critical cyber and communications networks and infrastructure of a nation. This comparison to a number of other threats, including violence and natural disasters. Public-private cooperation is particularly important in countries where the private sector is responsible for controlling or assuming responsibility for a given asset or system. In some countries, such as the U.S., the private sector accounts for 85% of critical infrastructure.The need for increased cyber security was evidenced by ongoing cyber intrusions into critical infrastructure.Nonetheless, it is essential to understand that these attacks often do not differentiate between the public and private sectors, and most often describe the effect on both industries. In the face of cyber threats, the nation's national and economic security depends on the reliable functioning of critical infrastructure. Critical Information Protection Infrastructure (CIIP) specifically refers to the measures necessary to protect IT systems. Like critical infrastructure, critical information infrastructure function degradation or loss may have disproportionate implications for national security.

Commonly employed techniques of carrying out attacks on critical information resources include: attempting to enter networks to obtain unauthorized access to information; modifying (or ' defacing') information on vulnerable websites or databases; performing ' silent operations ' (passively gathering information, not detected) and; large-scale assaults (such as DDoS or Ransomware). If we look into recent attacks on CII and or SCADA systems, we will find a disturbing situation. Any probable attack on critical infrastructure can be deadly and expensive. From the 2010 STUXNET to 2012 Saudi ARAMACO Wiper attack to 2015 Ukrain national power grid attack or 2016 Triton Attack, on all cases industrial control systems were targeted. On March 19, Norsk Hydro had to stop some of its production and switch other units to manual operation after hackers had ransomware blocked their systems. The financial impact was estimated at between 300 million and 350 million Norwegian crowns ($35 million-$41 million) during the first week on a preliminary basis.

To protect CII, we have to consider three basic things: Identifying what needs to be protected, identifying the relevant threats to your identified assets, Developing cost effective solutions for protecting them. We have to understand the difference between core IT System and Control system. In IT System CIA triad is present which elaborates to Confidentiality, Integrity and availability. But in SCADA and other industrial control systems SAIC is applicable which is Safety, Availability, Integrity & Confidentiality. When we are protecting such kind of systems, we have to work closely with Engineers and consider them as a valuable resource as they understands those control systems better than an IT person. To design any Control system, we have to follow applicable standards ISO/IEC 62443, IEC61502, NIST 800-82 etc.

Policymakers should strengthen critical infrastructure security and resilience and preserve a digital climate that facilitates efficiency, development, and economic prosperity while preserving security, security, customer secrecy, privacy, and civil liberties. Such goals can be accomplished by clearly defining what comprises critical infrastructure, through forming relationships with critical infrastructure owners and operators to enhance the sharing of information on safety, and by designing and enforcing risk-based principles in cooperation