Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Protecting Industrial Control Systems

JULY 2018

Introduction

Industrial control systems are essential to our daily life. They control the water we drink, the electricity we rely on and the transport that moves us all. It is critical that cyber threats to industrial control systems are understood and mitigated appropriately to ensure essential services continue to provide for everyone.

Providing cyber security for industrial control systems present several unique challenges, including:

- lack of security in engineering protocols
- the need to retest engineering systems after upgrades
- long lifecycles (20 to 50 years)
- the addition of many IT protocols, such as the Network Time Protocol and Address Resolution Protocol, to the engineering environment
- devices may not be set up to receive or respond to messages from standard IT debugging and analysis tools.

Understand your threat environment

Before appropriate mitigation strategies can be chosen, you must understand:

- Who might target your organisation?
- What particular infrastructure might they target?
- How bad could the impact from an attack on each of the parts of your infrastructure be?

Threat modelling your organisation will help answer some of these questions to identify what systems are critical for delivering essential services, and will allow you to appropriately set priorities and budget for cyber security activities.

Essential mitigation strategies

Below are essential mitigation strategies you can implement to protect your industrial control systems from a range of cyber threats. Use them where appropriate based on the outcomes of threat modelling activities:

- Tightly control or prevent external access to the industrial control system network. Segregate it from other networks such as the corporate network and the internet.
- Implement multi-factor authentication for privileged accounts and access originating from corporate or external networks.

- Disable unused external ports on devices.
- Visibly mark authorised devices inside the industrial control system environment with unique anti-tamper stickers.
- Make regular backups of system configurations and keep them isolated. Test the restoration procedure and validate the backup integrity periodically.
- Regularly review firewall settings are in an expected state.
- Prevent devices inside the industrial control system network from making connections to the corporate network or the internet.
- Enable logging on devices and store logs in a centralised location. Institute regular monitoring and incident response practices to ensure that anomalies are identified, investigated and managed in a timely fashion.
- Define a process for introducing software and patches into the industrial control system. Where necessary (e.g. on exceptionally critical components), review code and only allow approved binaries.
- Use vendor-supported applications and operating systems, and patch associated security vulnerabilities in a timely manner.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

For further guidance on protecting industrial control systems, see the following documents:

- The United States' National Security Agency's ***Seven Steps to Effectively Defend Industrial Control Systems*** at https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/industrial-control-systems/seven-steps-to-effectively-defend-ics.cfm.
- The United States' Department of Energy's ***21 Steps to Improve Cyber Security of SCADA Networks*** at https://www.hsdl.org/?abstract&did=1826.
- The National Institute of Standards and Technology's Special Publication 800-82 Rev. 2, ***Guide to Industrial Control System (ICS) Security***, at https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).