Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Protecting industrial control systems

First published: 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 cyberthreats to industrial control systems are understood and mitigated appropriately to ensure essential services continue to provide for everyone.

Providing cybersecurity 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 cybersecurity activities.

Essential mitigation strategies

Below are essential mitigation strategies you can implement to protect your industrial control systems from a range of cyberthreats. 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 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 vulnerabilities in a timely manner.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

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

- The United States' Cybersecurity & Infrastructure Security Agency's *Seven Steps to Effectively Defend Industrial Control Systems*.

- The United States' Department of Energy's *21 Steps to Improve Cyber Security of SCADA Networks*.

- The National Institute of Standards and Technology's Special Publication 800-82 Rev. 2, *Guide to Industrial Control System (ICS) Security*.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate