Quick Industrial Security Assessment
Key Concerns of Control System Security

1. Preventing accidental and unintentional changes to the control system by employees or others given authorized access to a system
2. Protecting against malicious threats that disrupt or damage system operation, affecting OEE
3. Protecting IP and know-how. Protecting your investments from imitators
4. Complying with emerging global standards such as ISA S99 and IEC-62443 to help drive commonality, consistency and standards of operation within control systems at risk
5. Influence from agencies such as US Department of Homeland Security to encourage, regulate and legislate standards of operation for Critical Infrastructure processes (Oil & Gas, Energy & Power, Water / wastewater, Transportation, and Chemicals)
How Secure Is Your System?

• Who has access to your industrial equipment?
  A. Pretty much everyone
  B. Anyone with a badge that provides access to our location
  C. Only individuals with a key to our control system panels
  D. Only trained individuals with a badge, keys and remote access

• What kind of firewalls and intrusion prevention systems do you use?
  A. What’s a firewall or intrusion detection/prevention system?
  B. We have guards, gates and a badge system, but no firewall to help block intruders
  C. We have a firewall to help block intruders, but no physical security system such as guards, gates or a badge system
  D. We employ a depth-in-defense system which includes both physical and cyber security mechanisms to control access to and protect critical systems and components
How Secure Is Your System?

• How often do you patch and update your system and components?
  A. Never
  B. We patch and update when we get around to it
  C. We patch and update hardware and software occasionally
  D. We follow a regular schedule for patching and updating our system and components according to our control system supplier’s recommendations

• How do you manage passwords?
  A. We don’t use passwords, or we use only default passwords
  B. Everyone uses the same password for simplicity sake
  C. We assign everyone a password at orientation and never change them again
  D. We have a system that prompts us to change passwords frequently
How Secure Is Your System?

How many of your controllers are in PROGRAM mode (PROG) or REMOTE RUN (REM RUN)?

A. Who knows, who cares? Does it matter what mode my controllers are in?
B. Probably about half, but I’m not sure which half
C. Only those that are being programmed or have been programmed recently
D. None. We have standard procedures to put controllers into RUN mode once all programming is completed. We also remove keys and lock cabinet doors.
How to Score

Score your answers as follows:

• 0 points for all A answers
• 1 point for all B answers
• 2 points for all C answers
• 3 points for all D answers

15 points
Congratulations, you are practicing the 5 basic steps to industrial security.
Do you know there are additional ways to enhance your industrial security?

14 to 12 Points
You’re better than many. You’re following most of the 5 basic steps to industrial security, but you could be doing more.
Ask Rockwell Automation what else you can do to enhance your industrial security.

Less than 12 Points
Whoa! Your systems may be seriously vulnerable to security threats.
Help is available! Talk to your Rockwell Automation representative NOW to learn 5 basic steps to enhance your industrial security.
Industrial Security Key Points

- Industrial security affects all industries
- Practice 5 simple, actionable steps to enhance industrial security:
  1. Control who has access
  2. Employ firewalls and intrusion detection/prevention
  3. Patch and update your system
  4. Manage your passwords
  5. Turn the processor key(s) to Run mode

- We strive to be our customer's number one security partner
- We provide free resources to help:
  - www.rockwellautomation.com/security
  - www.ab.com/networks/architectures.html
- We offer Network & Security Services to help you comply with security-oriented regulations and standards
  www.rockwellautomation.com/services/security/

Enhance industrial security to better protect IP, OEE and help prevent attacks
Why Is Rockwell Automation Different?

1. We have the unique capability of connecting Process Control and Discrete Control systems together and help link these into larger enterprise-level systems.
Why Is Rockwell Automation Different?

2. We address industrial security from a system approach throughout the Integrated Architecture and align with reputable global standards.

Many competitors promote products as fragmented pieces of a secure system.
Why Is Rockwell Automation Different?

3. We have adopted specific design-for-security development practices into our product and system development process.
Why Is Rockwell Automation Different?

4. We continue to expand the physical, cyber and IP protection mechanisms in control products to simultaneously advance the security and safety of the industrial control system.

We have unprecedented responsiveness in patch validation, incident remediation and open and timely communication with customers.
5. We cultivate relationships with network infrastructure vendors like Cisco and other security-enabling Encompass™ partners to enhance industrial security and provide guidelines, recommendations and practical advice for reducing operational risk.

Detailed recommendations can be found in the Rockwell Automation-CISCO co-authored Reference Architectures for Manufacturing Design and Installation Guide (DIG2.0) available at www.ab.com/networks/architectures.html.
6. We offer experienced field consulting services to assess, recommend and help implement solutions that enhance control system security.
Why Is Rockwell Automation Different?

1. We connect Process Control and Discrete Control systems together and help to link these into larger enterprise-level systems
2. We address industrial security from a system approach throughout the Integrated Architecture
3. We have adopted specific design-for-security development practices into our product and system development process
4. We continue to expand the physical, cyber and IP protection mechanisms in control products to simultaneously advance the security and safety of the industrial control system
5. We cultivate relationships with network infrastructure vendors and partners to enhance industrial security
6. We offer experienced field consulting services to assess, recommend and help implement solutions that enhance control system security

We address product and control system risk and help reduce risk to the enterprise