Cybersecurity Essentials for Smart Manufacturing Professionals

Module 3: Configuration Management and Maintenance

ESL Global Cybersecurity Institute

Rochester Institute of Technology

September 2023

Learning Outcomes

By the end of this class, you will be able to:

- ❑ Understand the importance of configuration management
- ❑ Understand the basics of wireless networks used in Industrial Internet-of-Things
- ❑ Understand the importance of regular updates and monitoring
- ❑ Understand the importance of cloud-based backup and recovery
- ❑ Identify best practices for secure maintenance

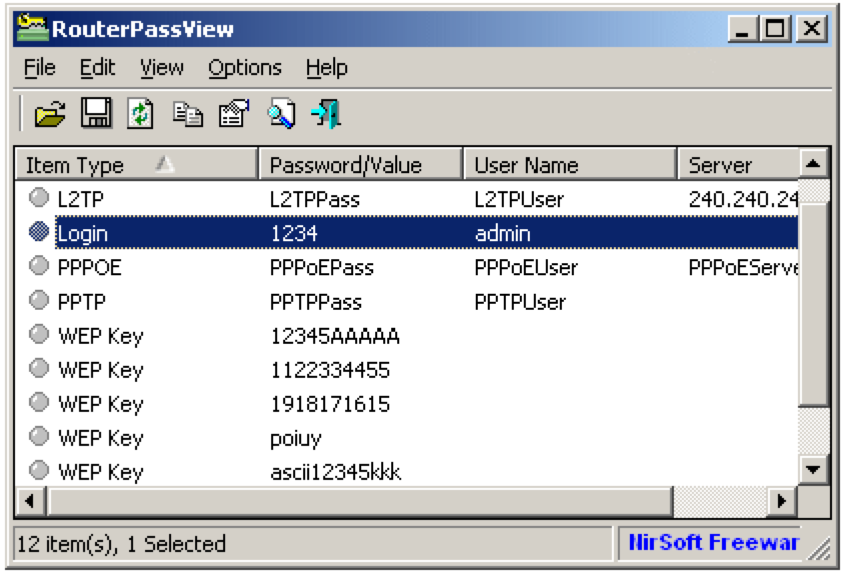
Configuration Management

Configuration Management

- ❑ What do you know about configuration management?
- ❑ Why do you think we should care?
- ❑ Configuration Management Definition
  - Adjusting default settings to increase security and mitigate risk
    - Recall – risk defines the likelihood of an attack and its impact
- ❑ Importance
  - Mitigate simple attacks that target default configurations
  - Identify misconfigurations that may have a severe impact

Examples of bad configurations

- Default passwords can be very easily exploited.
  - CNC machine user accounts
  - Wi-Fi networks
  - Cloud-based accounts
- Sometimes there is no password at all!
  - Example, Wi-Fi Open Networks



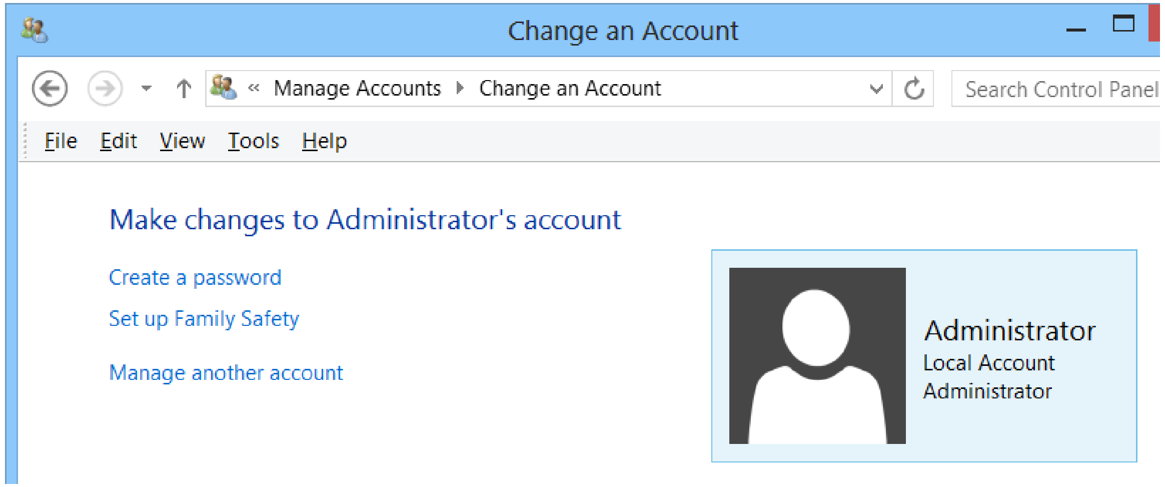
Item Type	Password/Value	User Name	Server
L2TP	L2TPPass	L2TPUser	240.240.24
Login	1234	admin	
PPPOE	PPPoEPass	PPPoEUser	PPPoEServe
PPTP	PPTPPass	PPTPUser	
WEP Key	12345AAAAA		
WEP Key	1122334455		
WEP Key	1918171615		
WEP Key	poiuy		
WEP Key	ascii12345kkk		

12 item(s), 1 Selected

NirSoft Freewar

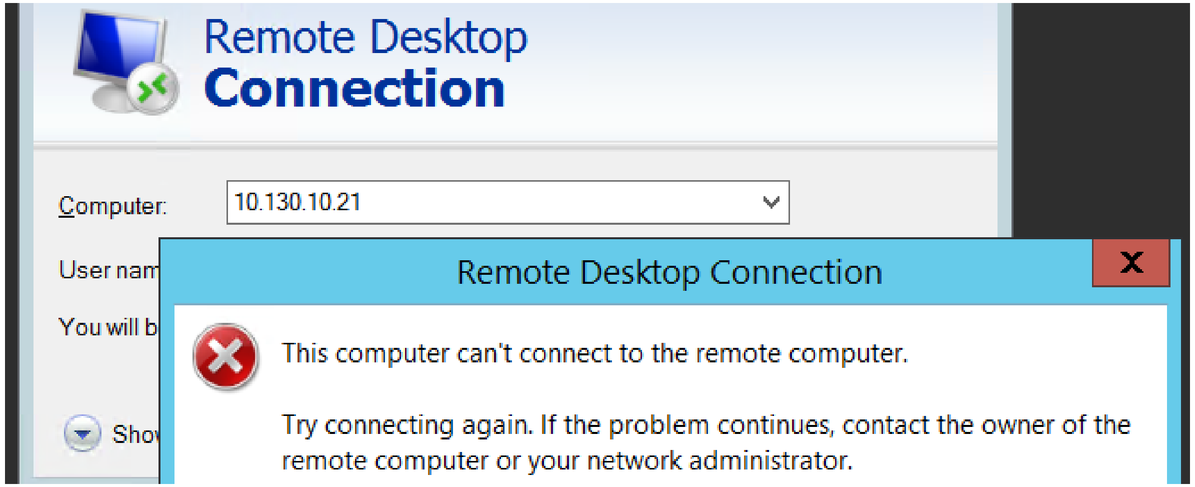
Examples of bad configurations

- Misconfigurations – settings that are usually more convenient for users, but bad for security. For example:
  - Activating the admin account to install insecure software
  - ***Reusing*** passwords across different accounts
  - Incorrectly configuring remote desktop to allow working from home



Make changes to Administrator's account

Administrator
Local Account
Administrator



Computer: 10.130.10.21

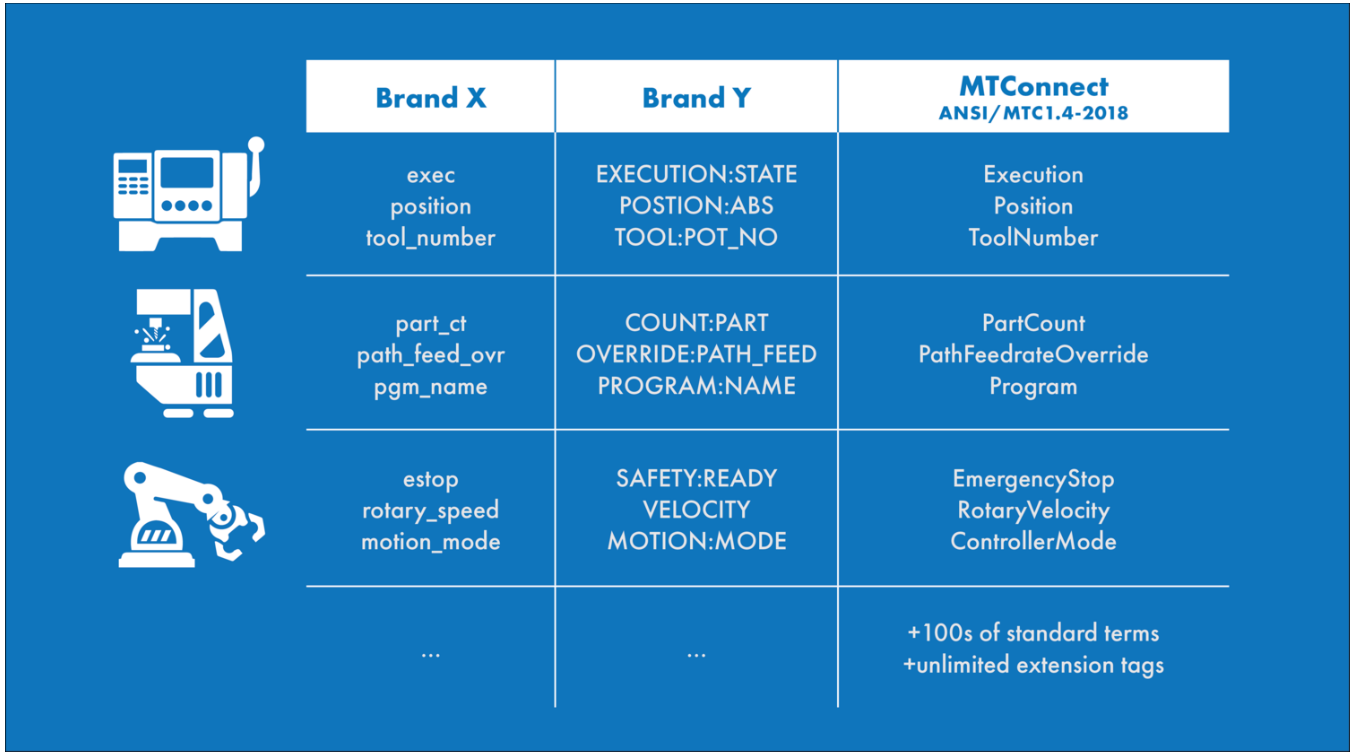
Remote Desktop Connection

This computer can't connect to the remote computer.

Try connecting again. If the problem continues, contact the owner of the remote computer or your network administrator.

MTConnect – Overview

- ❑ Provides semantic vocabulary standardization across machines
  - Latest standard – ANSI/MTC1.4-2018
- ❑ Convert data in proprietary formats from different brands

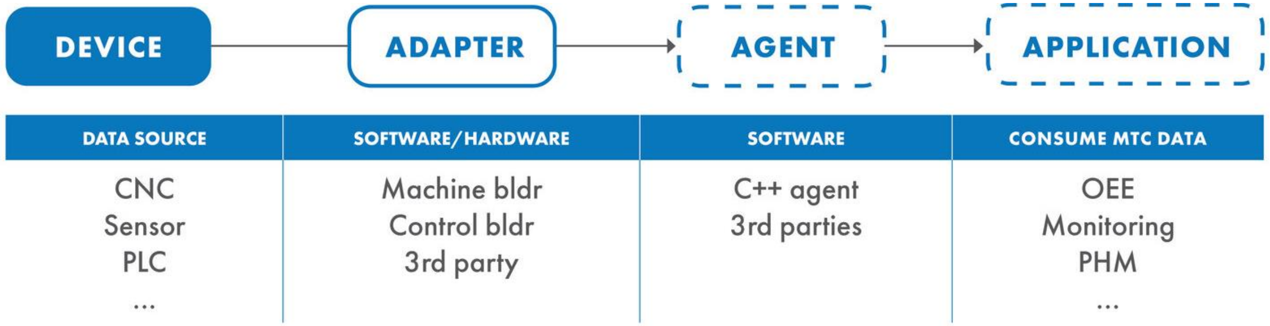


Brand X	Brand Y	MTConnect ANSI/MTC1.4-2018
exec position tool_number	EXECUTION:STATE POSTION:ABS TOOL:POT_NO	Execution Position ToolNumber
part_ct path_feed_ovr pgm_name	COUNT:PART OVERRIDE:PATH_FEED PROGRAM:NAME	PartCount PathFeedrateOverride Program
estop rotary_speed motion_mode	SAFETY:READY VELOCITY MOTION:MODE	EmergencyStop RotaryVelocity ControllerMode
…	…	+100s of standard terms +unlimited extension tags

mtconnect.org

MTConnect – Operation

- CNC machines from different manufacturers use different formats for presenting and configuring data
- MTConnect stores CNC machine operational data, such as status, tool data, and error codes
  - A software adapter translates the proprietary languages.
  - An agent aggregates and presents the data in readable format

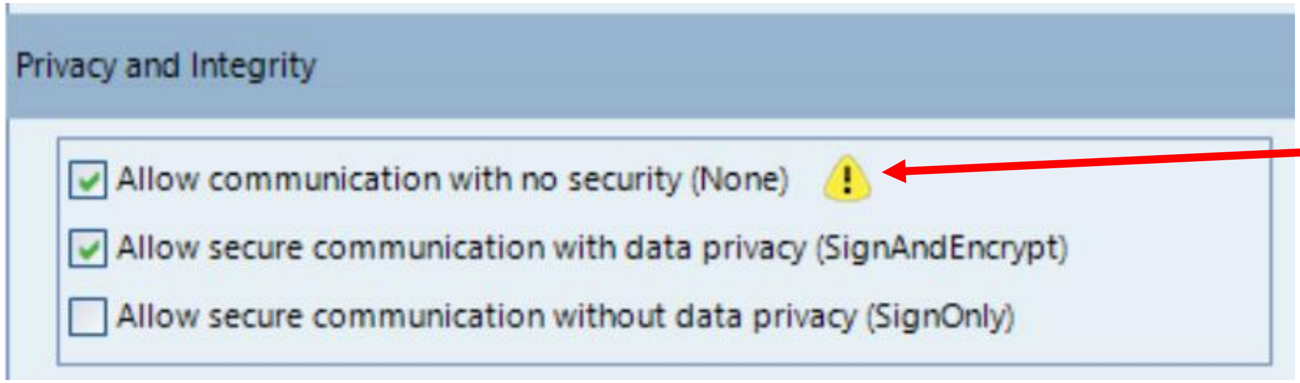


DEVICE	ADAPTER	AGENT	APPLICATION
DATA SOURCE	SOFTWARE/HARDWARE	SOFTWARE	CONSUME MTC DATA
CNC Sensor PLC ...	Machine bldr Control bldr 3rd party	C++ agent 3rd parties	OEE Monitoring PHM ...

mtconnect.org

MTConnect – Secure Configuration

- Ensure all data communication allows data privacy.



Privacy and Integrity

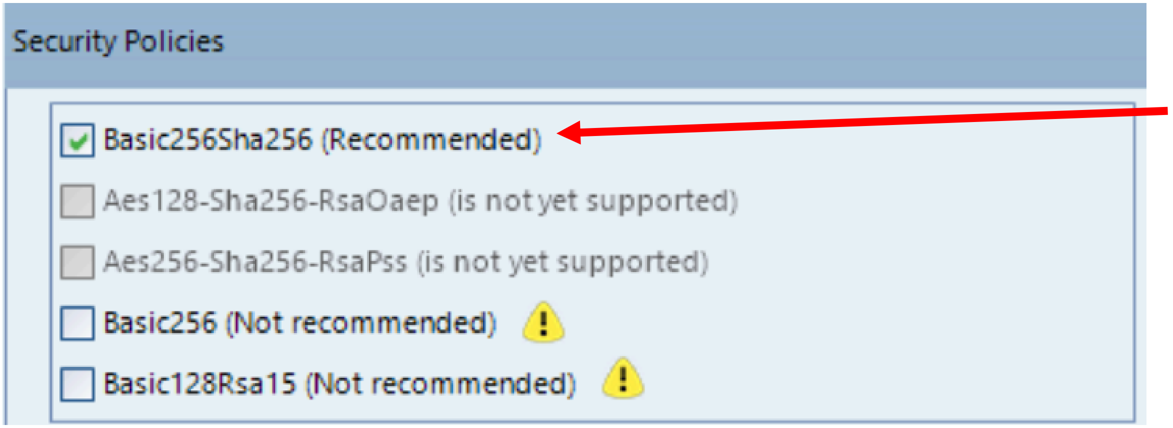
☑ Allow communication with no security (None) ⚠

☑ Allow secure communication with data privacy (SignAndEncrypt)

☐ Allow secure communication without data privacy (SignOnly)

Uncheck this!

- Ensure recommended settings for security policies



Security Policies

☑ Basic256Sha256 (Recommended)

☐ Aes128-Sha256-RsaOaep (is not yet supported)

☐ Aes256-Sha256-RsaPss (is not yet supported)

☐ Basic256 (Not recommended) ⚠

☐ Basic128Rsa15 (Not recommended) ⚠

Uncheck this!

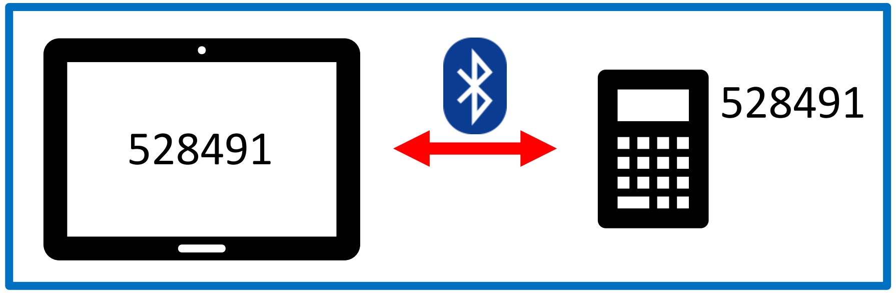
Wireless Networks used in Industrial Internet-of-Things

Industrial Internet-of-Things (IIoT)

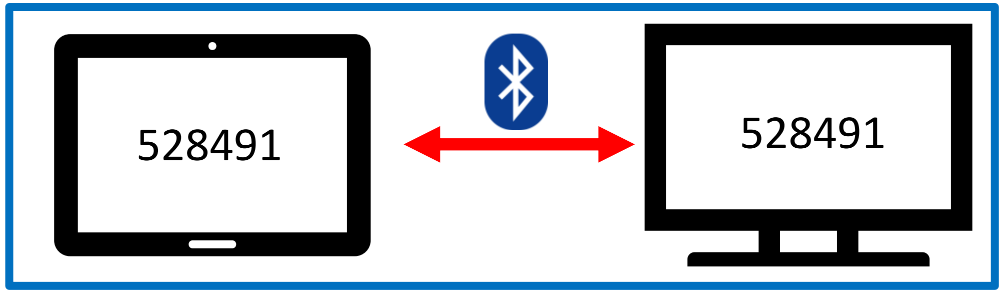
- Using wireless devices and computing to improve machining.
  - Remote monitoring
  - Logistics management
  - Employee safety
  - Machine automation
  - **AR/VR-aided manufacturing**

Bluetooth

- Portable personal area network
  - Transfer files, stream audio, control multimedia systems
- Recommended Bluetooth pairing methods
  - Passkey entry – number displayed on one device which is entered on another
  - Numeric comparison – compare numbers on two devices



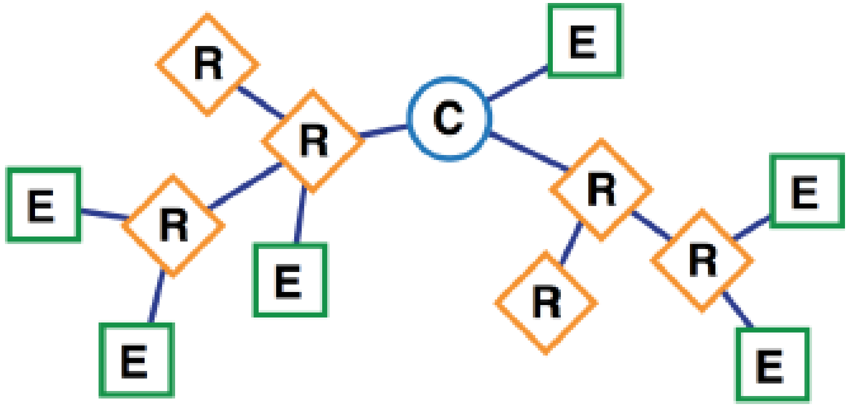
Passkey entry



Numeric comparison

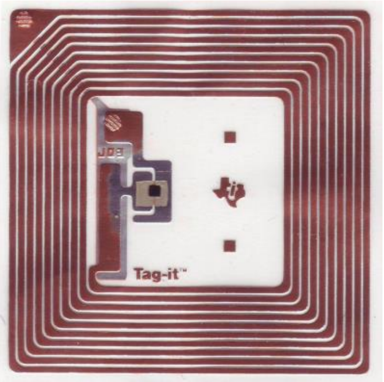
ZigBee and ZWave

- Low-power, short-range communication
  - Tool monitoring, automation, control systems
- Three types of devices
  - Coordinator (C) – manages security keys, typically a server
  - Router (R) – hub for end devices
  - End device (E) – sensors, etc.
- Required configuration steps
  - Change default passwords



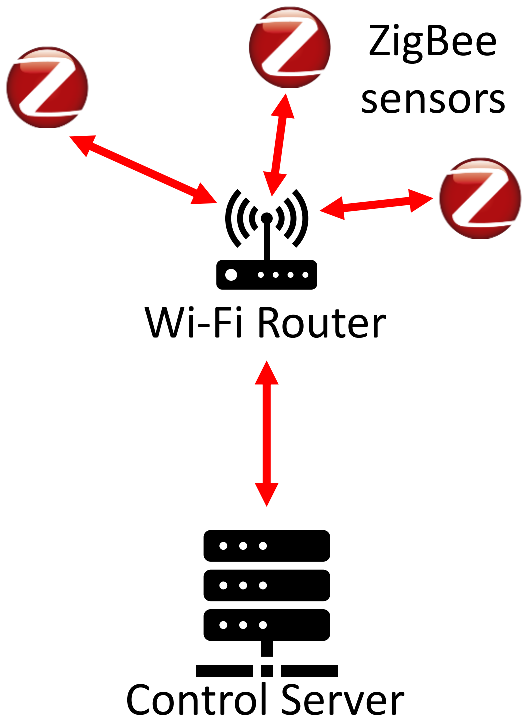
RFID and NFC

- Radio-frequency Identification (RFID)
  - A tiny radio tag to store and transmit an identifying number
  - Used in vibration sensors
- Near-field Communication (NFC)
  - Extremely short range
  - Used for payments, pairing, etc.

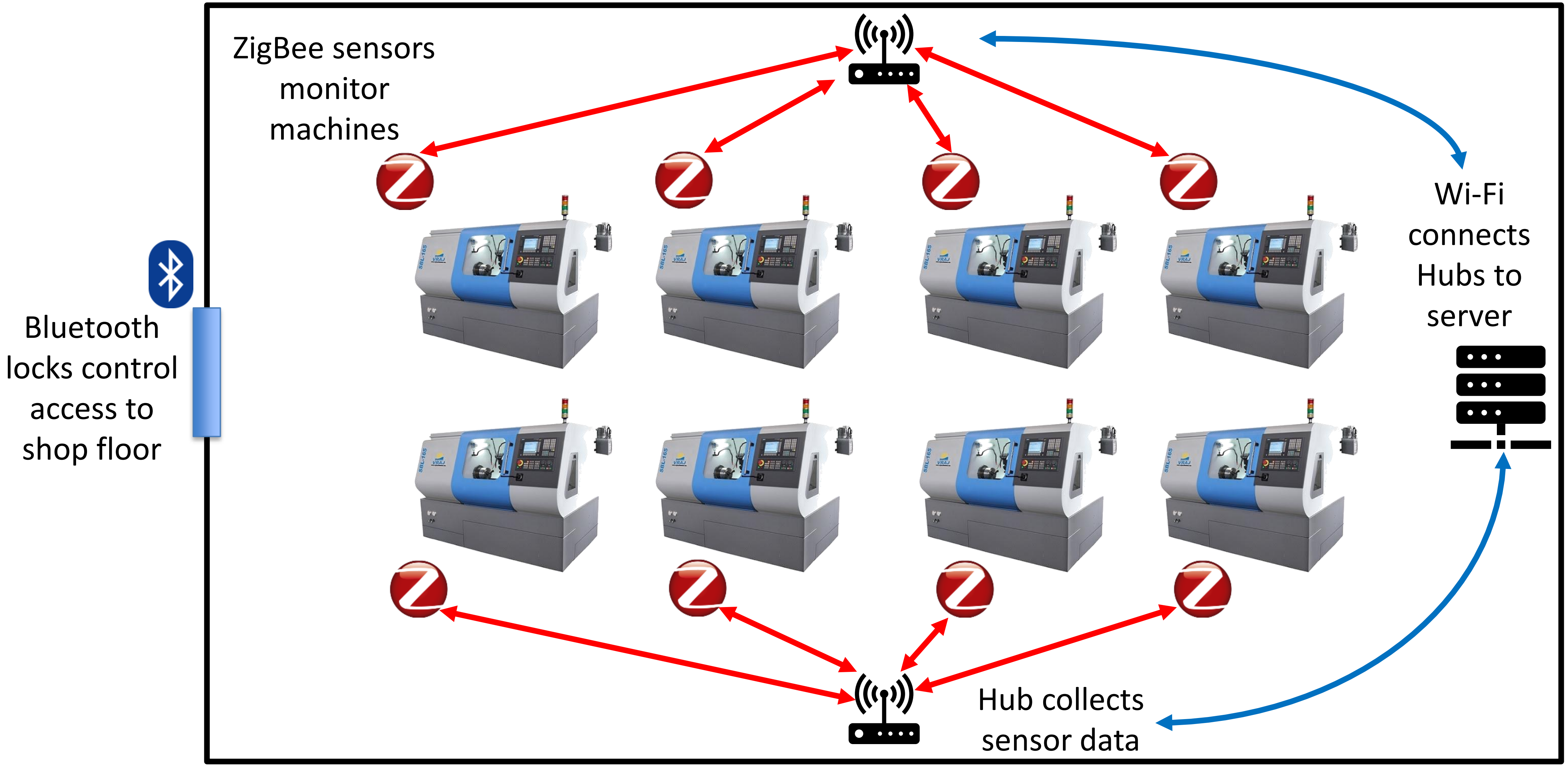


Wi-Fi

- Wireless networks for high-speed data transfer over wide range
  - Used for connecting sensor hubs with other computing resources
- Recommended configurations for Wi-Fi
  - Change the default password!
  - Use WPA2 or WPA3 security modes
  - Use unique passwords for different networks
  - Periodically update Wi-Fi router firmware



Example IIoT network in CNC Shop floor



ZigBee sensors monitor machines

Wi-Fi connects Hubs to server

Bluetooth locks control access to shop floor

Hub collects sensor data

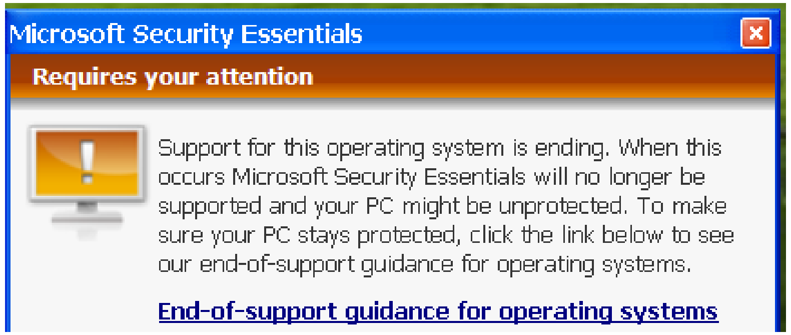
Importance of Regular Updates and Maintenance

Understanding our Mindset on Updates

- Why do we rarely update our software?
- We regularly maintain our car, why not our software?
- There are legitimate reasons for not updating regularly
  - OS updates, especially Windows, can be inconvenient.
  - Windows update can cause computer slowdowns.
  - Many companies still use legacy software which only works on certain OS versions.
- Maintenance can be expensive for complex organizations
  - Heavy reliance on legacy systems is a big deterrence.

Updating OS is Critical for Security

- 62% of smart manufacturing machines have outdated OS. Many popular Windows versions are no longer supported:
  - Windows XP – April 2014
  - Windows 8 – January 2016
  - Windows 7 – January 2020



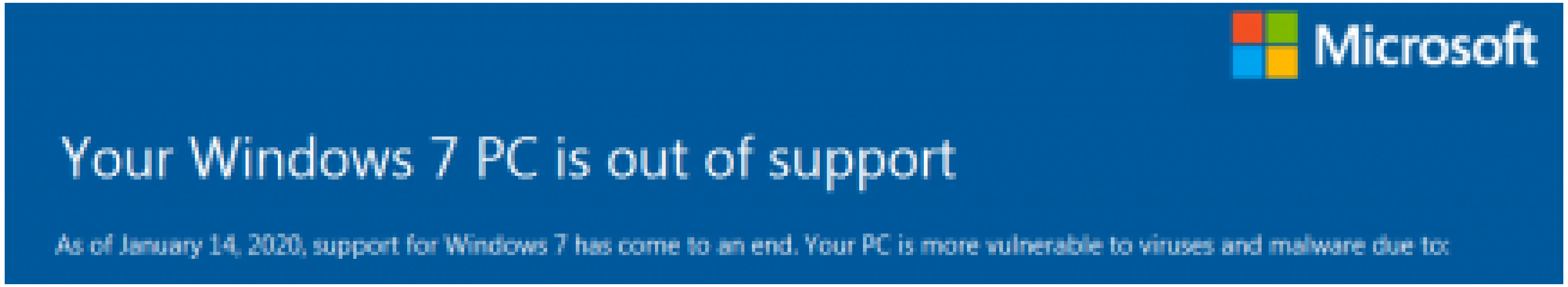
Microsoft Security Essentials

Requires your attention

Support for this operating system is ending. When this occurs Microsoft Security Essentials will no longer be supported and your PC might be unprotected. To make sure your PC stays protected, click the link below to see our end-of-support guidance for operating systems.

End-of-support guidance for operating systems

- Lack of support means no more security updates!
  - Very easy targets for attacks that can no longer be mitigated



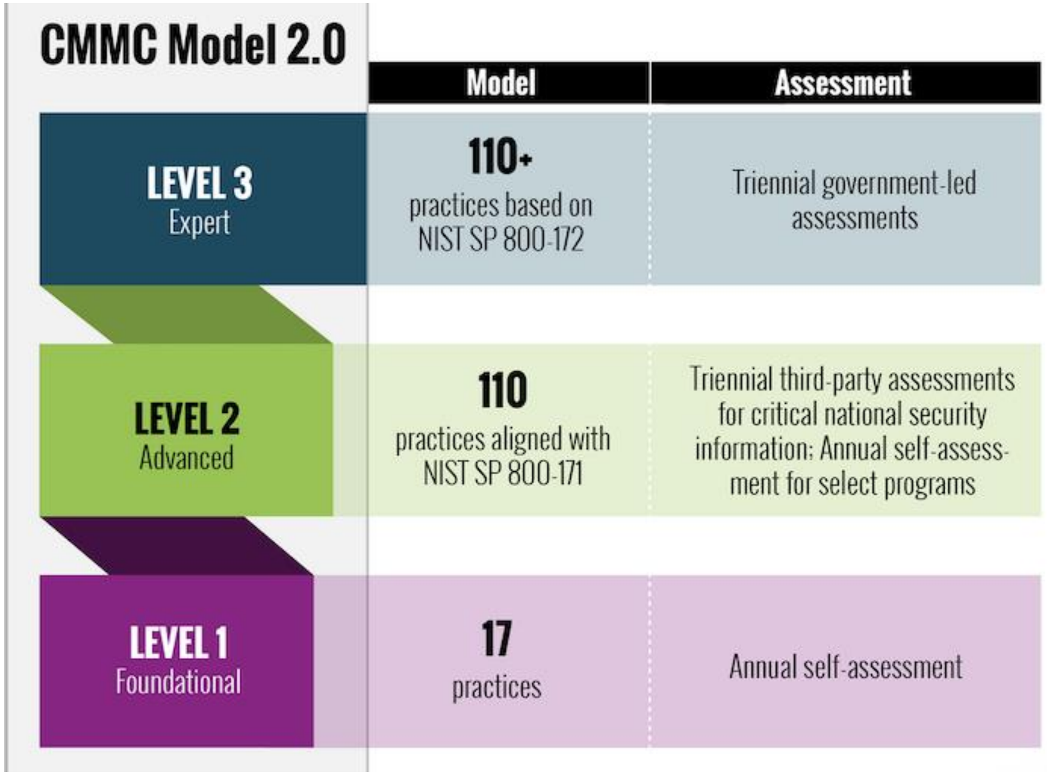
Microsoft

Your Windows 7 PC is out of support

As of January 14, 2020, support for Windows 7 has come to an end. Your PC is more vulnerable to viruses and malware due to:

Compliance with Industry Standards

- Cybersecurity Maturity Model Certification (CMMC)
  - Required for U.S. Dept. of Defense contracts
  - Mandates regular government-led assessments
  - Constant updates required to remain compliant

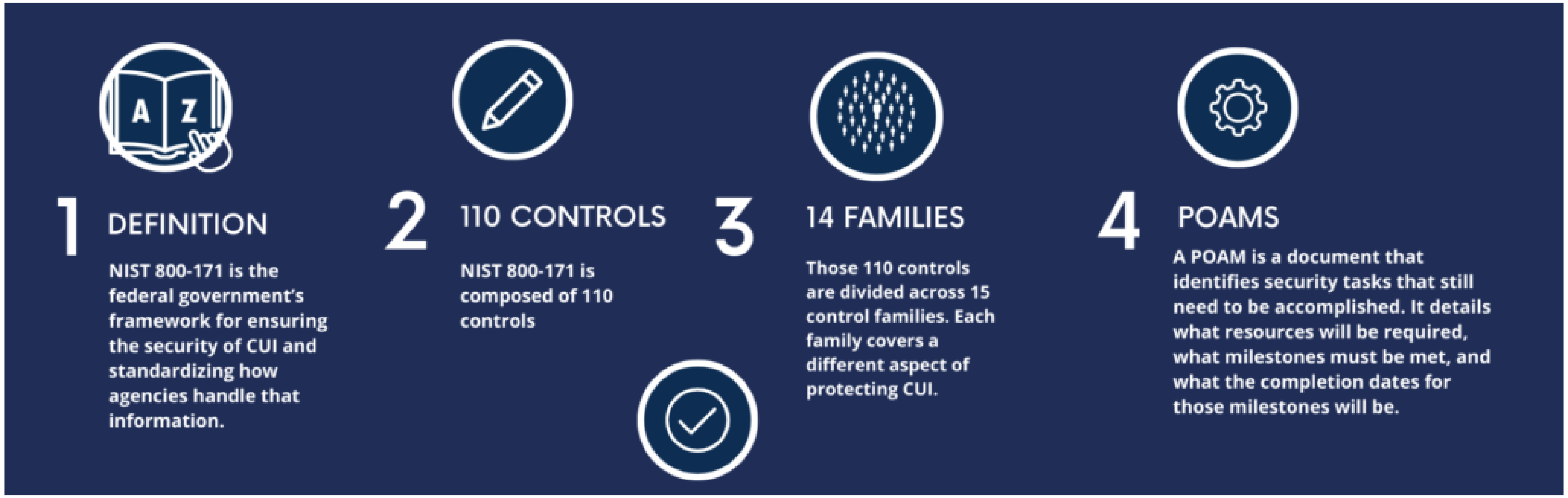


CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information: Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

Compliance with Industry Standards

- National Institute of Standards and Technology (NIST)
  - Special Publication 800-171 and 800-172 are relevant to machining
  - Specifies best practices and requirements for protecting controlled unclassified information
  - Compliance with NIST is required to be CMMC compliant



1 DEFINITION

NIST 800-171 is the federal government's framework for ensuring the security of CUI and standardizing how agencies handle that information.

2 110 CONTROLS

NIST 800-171 is composed of 110 controls

3 14 FAMILIES

Those 110 controls are divided across 15 control families. Each family covers a different aspect of protecting CUI.

4 POAMS

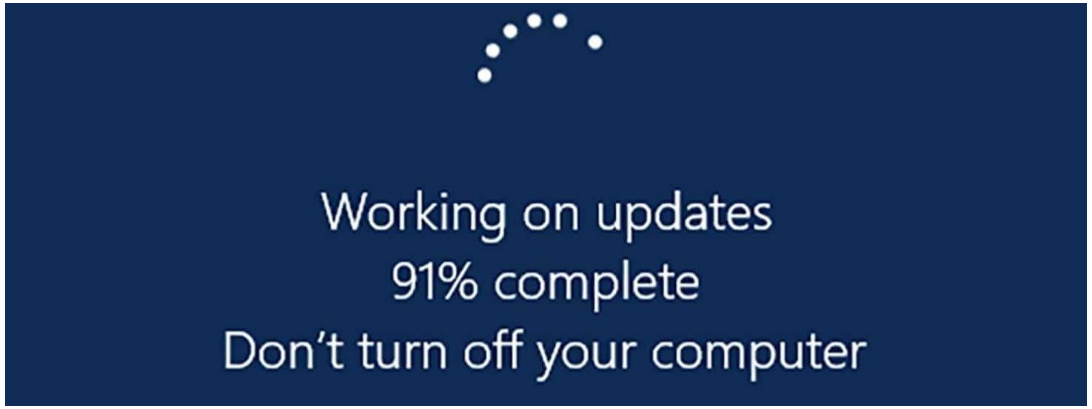
A POAM is a document that identifies security tasks that still need to be accomplished. It details what resources will be required, what milestones must be met, and what the completion dates for those milestones will be.

https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Monitoring Configurations and Updates

Monitoring Security Updates

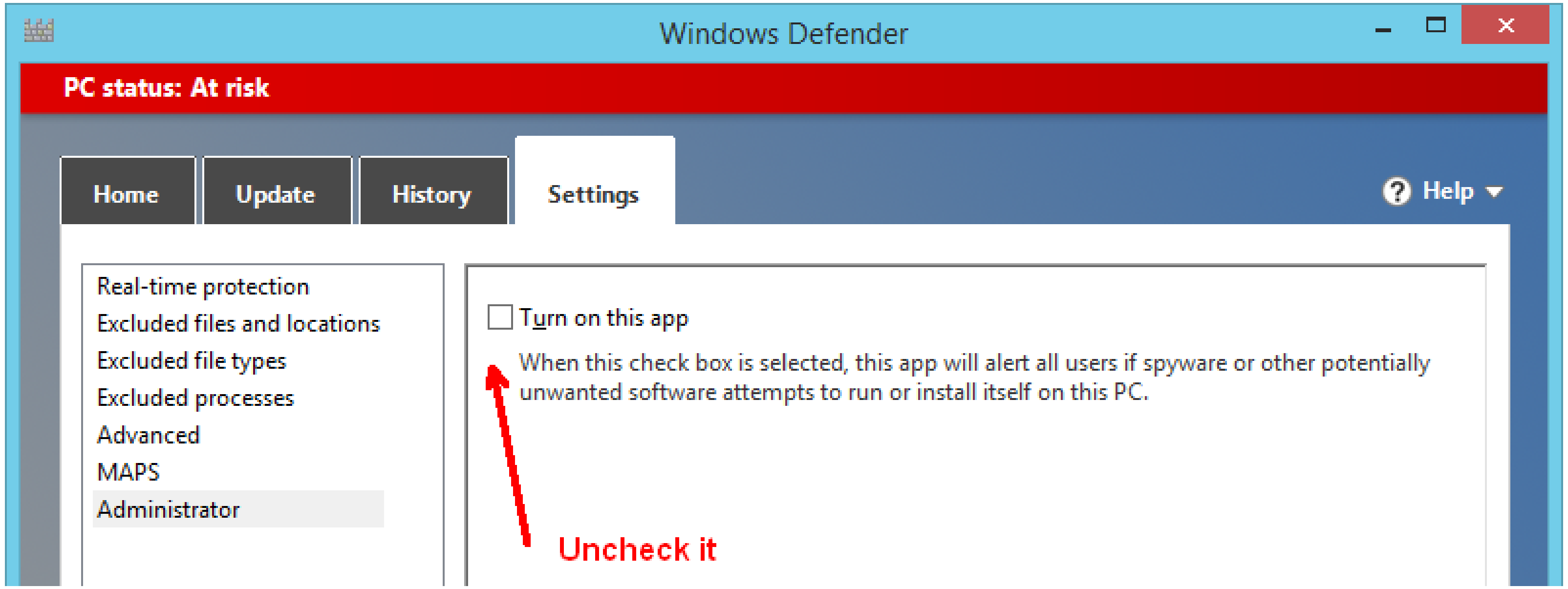
- ❑ Have you faced software bugs after performing updates?
- ❑ Some software updates may cause more harm than good
- ❑ Unnecessarily updating one software may create incompatibilities with another software
  - For example, a CNC machine tool application may only be compatible with certain versions of Windows.



Working on updates
91% complete
Don't turn off your computer

Monitoring Configuration Changes

- Misconfigurations done for a small amount of time need to be detected!
  - They may be a part of an attack – for example, disabling Windows Defender momentarily to install malware.



Windows Defender

PC status: At risk

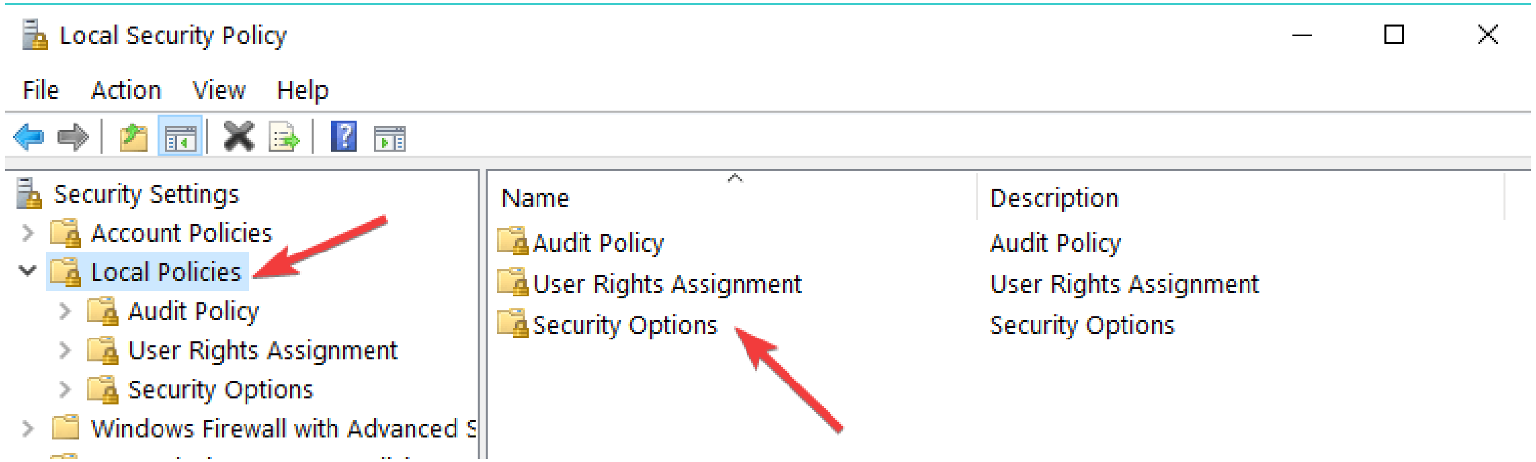
□ Turn on this app

When this check box is selected, this app will alert all users if spyware or other potentially unwanted software attempts to run or install itself on this PC.

Uncheck it

Monitoring Configuration Changes

- Misconfigurations can be easily detected using proper configuration monitoring. Example:
  - The Windows Group Policy provides settings to monitor configurations and alert on misconfigurations.
  - Alerts help identify the source of the misconfiguration and prevent an attack or malware from spreading to other machines.

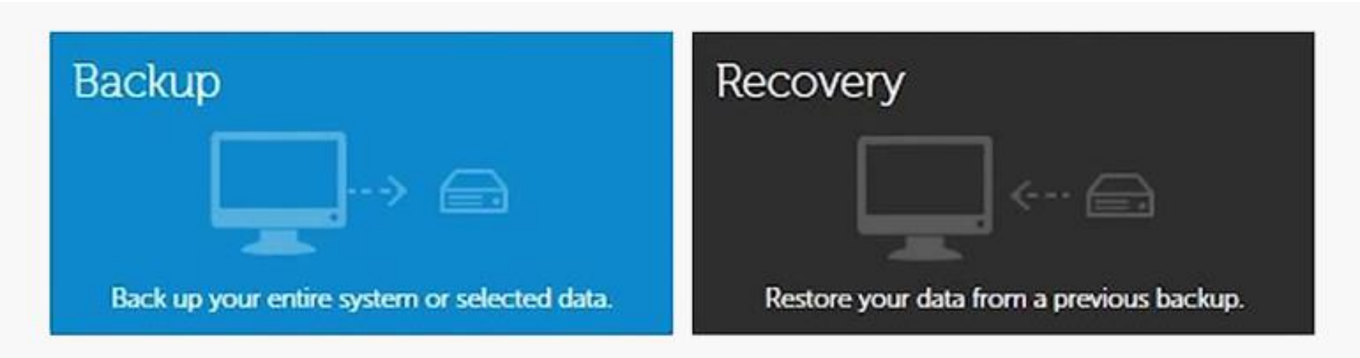


Name	Description
Audit Policy	Audit Policy
User Rights Assignment	User Rights Assignment
Security Options	Security Options

Cloud-based Backup and Recovery

Importance of Backup and Recovery

- Has anyone been a victim of natural disasters while on the shop floor? What was you experience like?
- In the event of attacks or natural disasters, it is important to ***maintain*** business continuity.
  - Attacks may take days or even weeks to investigate and mitigate
  - Natural disasters may severely cripple production lines.

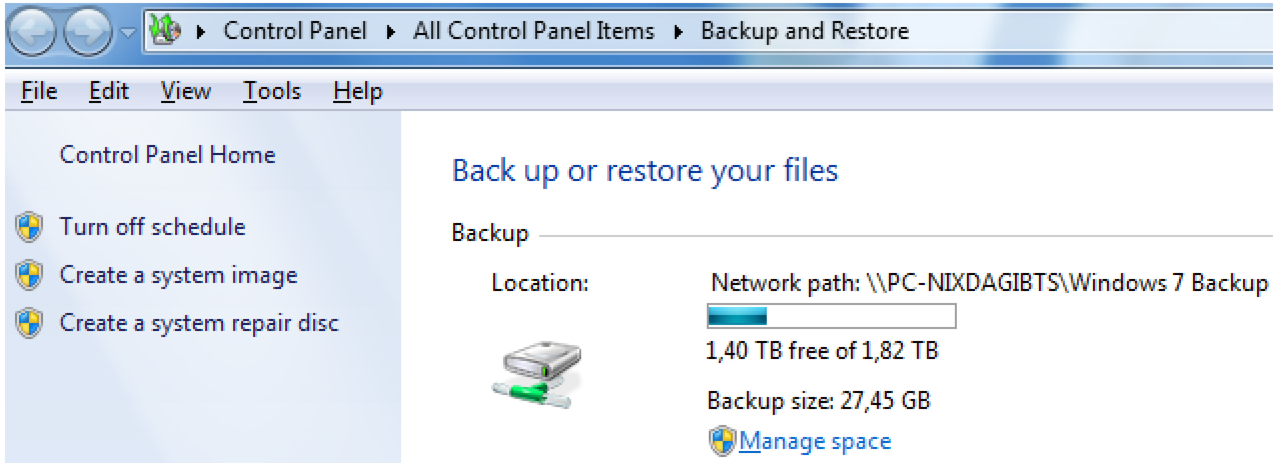


Back up your entire system or selected data.

Restore your data from a previous backup.

Backup and Recovery Processes

- Backup and Recovery is a part of regular maintenance.
- Backups are a copy of your digital user and company data.
  - Stored at a location far away from primary work address. (Why?)
  - Isolated from the primary network of machines and computers.
  - Updated monthly or quarterly depending on size of the company.


Control Panel ▸ All Control Panel Items ▸ Backup and Restore
File Edit View Tools Help
Control Panel Home
Turn off schedule
Create a system image
Create a system repair disc
Manage space

Back up or restore your files

Backup

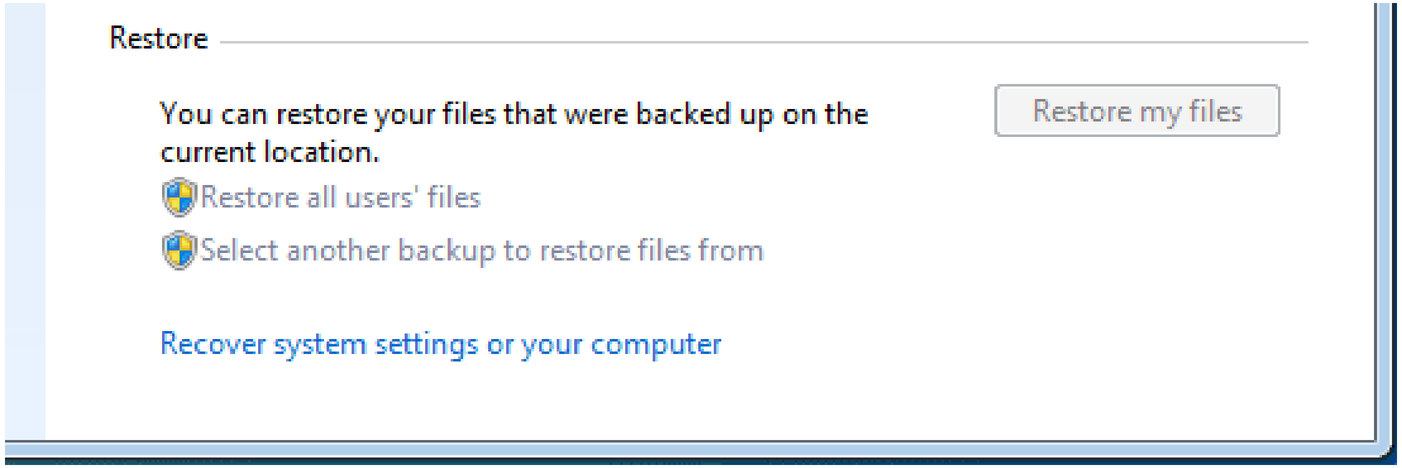
Location: Network path: \\PC-NIXDAGIBTS\Windows 7 Backup

1,40 TB free of 1,82 TB

Backup size: 27,45 GB

Backup and Recovery Processes

- Recovery is the process of restoring business operations
  - For example, a ransomware attack can be mitigated by restoring user and business data from backups.
  - If natural disasters cause significant damage to primary locations, recovery from backups ensures no data is lost.



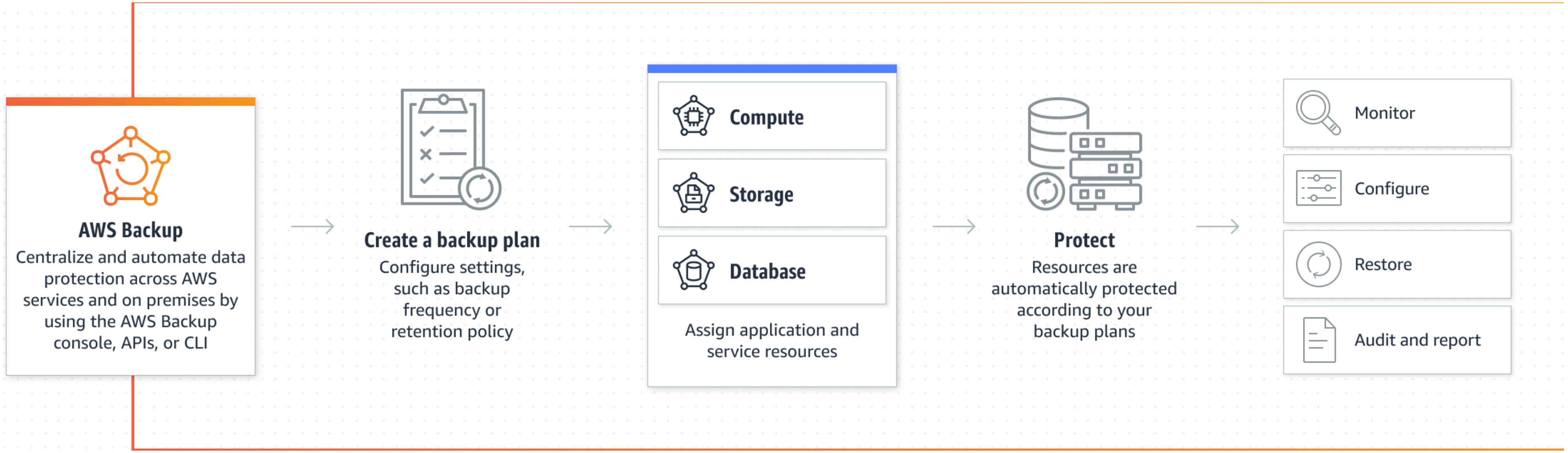
Restore

You can restore your files that were backed up on the current location.

Restore my files
Restore all users' files
Select another backup to restore files from
Recover system settings or your computer

Cloud-based Backup and Recovery

- Cloud-based services streamline and simplify the process of creating and managing backups
  - No need to store data at a secondary location, which reduces expenses.
  - Backups can be easily restored.


AWS Backup
Centralize and automate data protection across AWS services and on premises by using the AWS Backup console, APIs, or CLI
Create a backup plan
Configure settings, such as backup frequency or retention policy
Compute
Storage
Database
Assign application and service resources
Protect
Resources are automatically protected according to your backup plans
Monitor
Configure
Restore
Audit and report

Best Practices for Configuration Management and Maintenance

Best Practices for Configuration Management

- ❑ Always change default passwords when installing new software, user accounts or devices, such as:
  - New CNC machines
  - New IoT devices – Wi-Fi routers, ZigBee/ZWave sensors
- ❑ Never activate the admin account for installing new software
  - Request the IT department to check the integrity of software first
- ❑ Request IT to setup remote desktop features securely:
  - Only be accessible via user accounts that can be easily monitored
  - Limited remote upload/download of files to/from work machines

Best Practices for Software Updates

- Always cross verify whether software updates are stable, with no bugs, and are compatible with each other
  - Before making any updates, ensure that the update is stable and has no bugs. This will require investigation by the IT team.
  - Ensure that installed software is updated before updating the OS.
- Ensure that updates are performed during non-operational hours
  - Prevent any ongoing machining jobs from getting disrupted.
- Firmware updates should be performed very carefully as it can potentially cause physical damage if not done properly.
  - For example, ensure that there are no interruptions in power supply.

Best Practices for Cloud-based Backups

- ❑ Ensure that the security services of the cloud provider are compliant with machining security standards.
  - For example, NIST SP 800-171 and CMMC 2.0.
- ❑ Cloud services need to be secured with proper access control.
  - Only shop floor managers and supervisors can access backup data.
- ❑ Cloud data should be constantly monitored
  - If any attackers modify the backup data, it needs to be detected and alerted.

https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Thank you!

Contact: hanif.rahbari@rit.edu

Wireless and IoT Privacy (WISP) Lab (rit.edu/wisplab)

ESL Global Cybersecurity Institute

Rochester Institute of Technology

Hanif Rahbari

Sid Dongre