Cybersecure Plant Maintenance Procedures

MLM-37-A

Industry	– Process
Principal Role	– Owner
Professional Role	– All
Enterprise Phase	– Operations

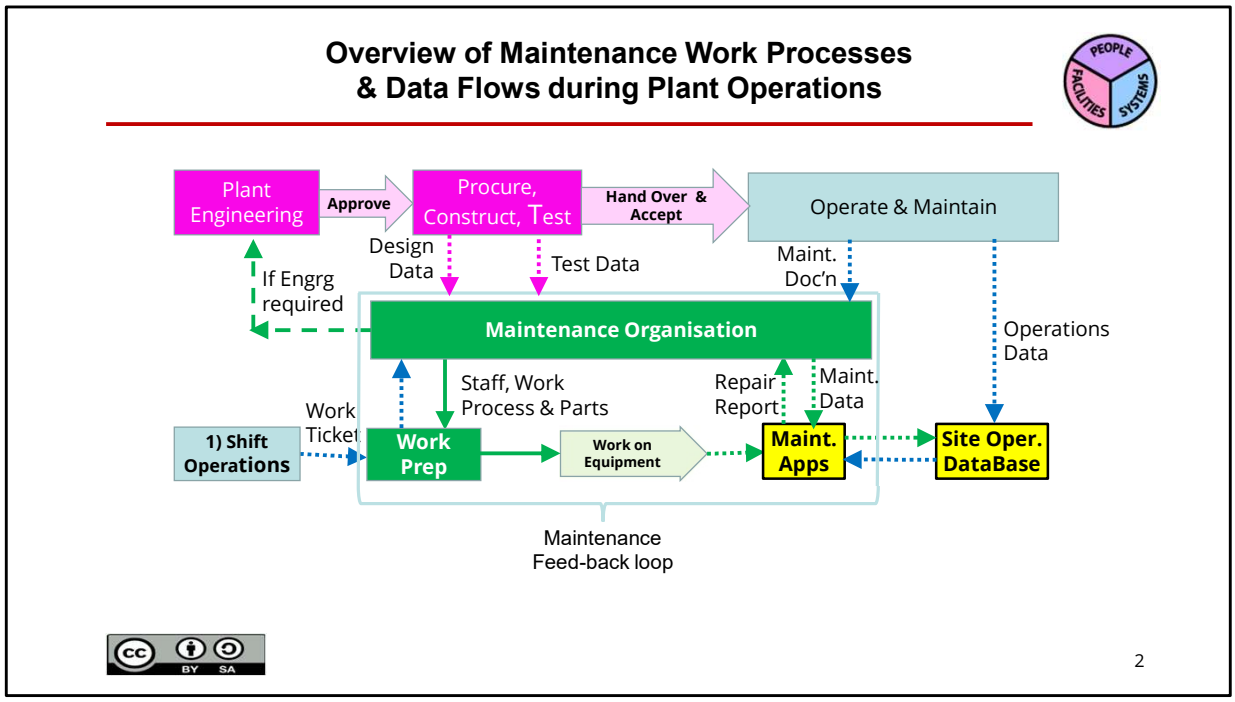
Turn on your audio and click start to begin video

START

Image is from PowerPoint Stock Images

This Micro-Learning Module describes plant maintenance practices to limit the risk from cybersecurity attacks. These practices are important in order to secure critical plant infrastructure. The basic approach in this MLM is to examine information flows during plant maintenance and identify where risks may be reduced and cybersecurity enhanced.

Click the START or NEXT button to advance to the next page.



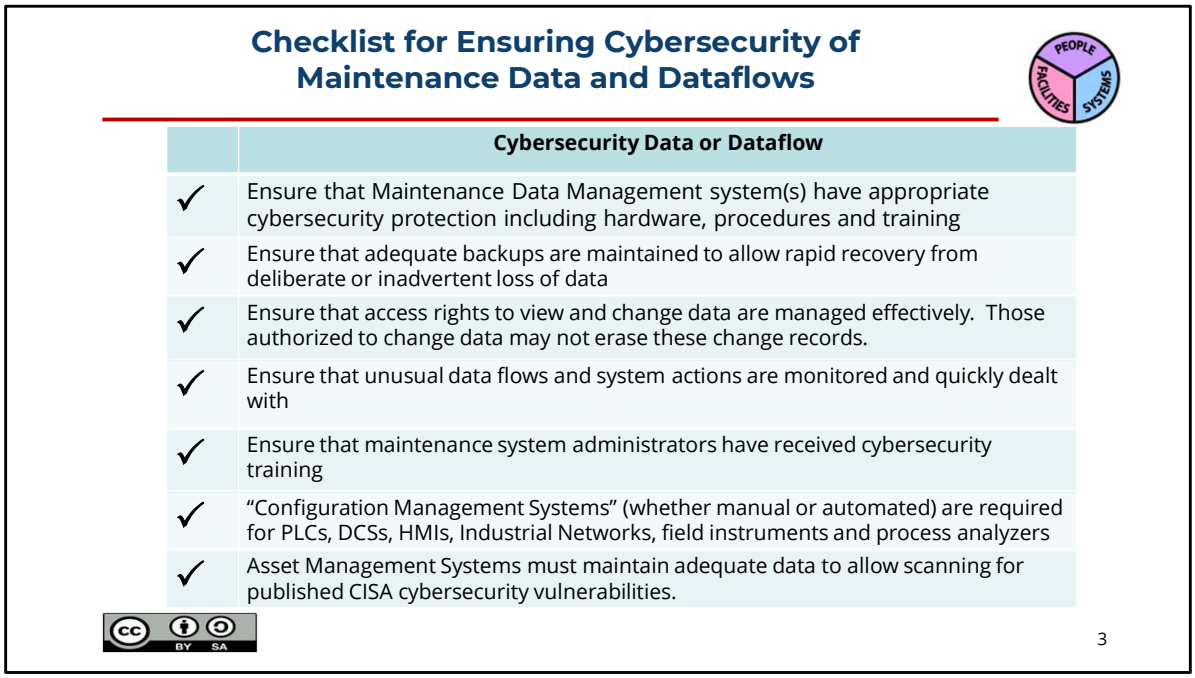
This diagram shows an overview of data flows during plant maintenance activities.

Cybersecurity must be part of each Work Process and involves all of the personnel, equipment, and software used.
Cybersecurity of the data, the networks, and the devices used must be considered for all of these data flows. That includes devices that carry data (and potentially viruses), including "thumb drives," industrial networks, hand-held programmers, tablets, and laptop computers.

Cybersecurity Learning Maps are being developed for Plant Production, Plant Engineering, Plant Procurement, and Plant Maintenance personnel. The purpose of these is to provide a high-level description of what each Professional Role must do to help establish and maintain the cybersecurity of ACS at a plant.

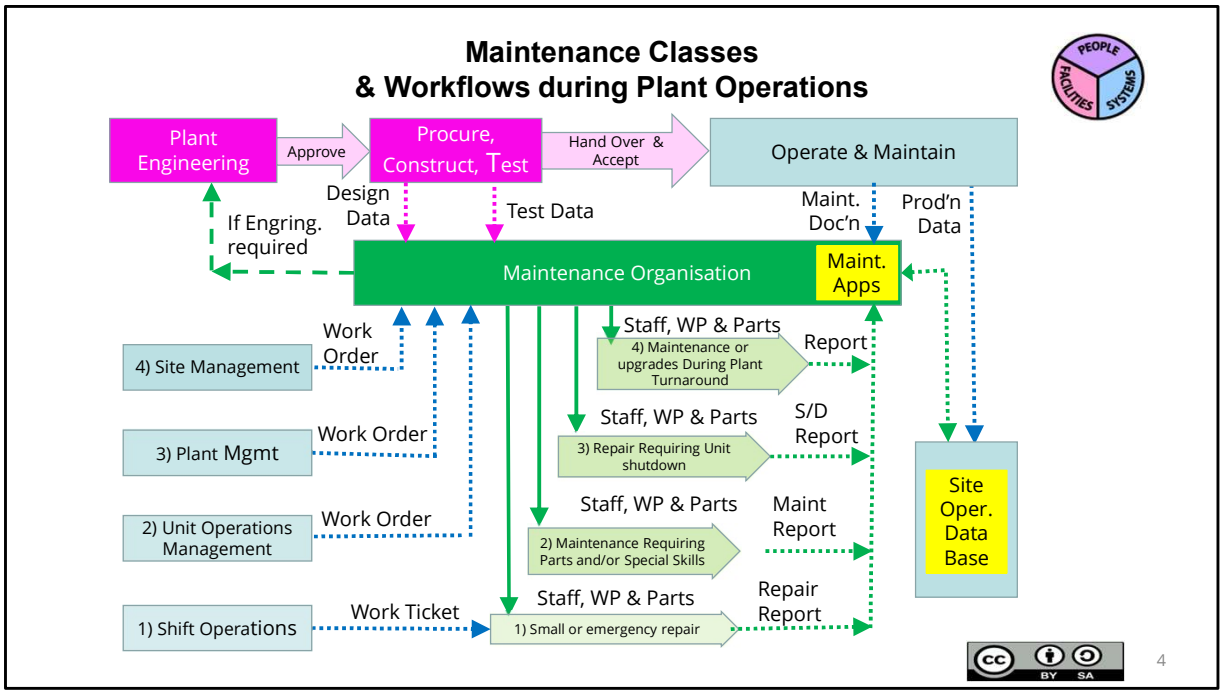
The maintenance feedback loop, including work processes and associated data flows are also shown here.

Plant Operations workflows and data are indicated in Blue, Maintenance in Green, Engineering and Construction in red. Systems provided by Plant IT are indicated in yellow.



This Cybersecurity checklist for a maintenance data management system (or MMS) is in addition to, and separate from, the checklists from each of the previous workflows.

Ensure that the Maintenance Data Management system(s) have adequate cybersecurity protection, including hardware, procedures, and training
Ensure that adequate backups are maintained to allow rapid recovery from deliberate or inadvertent loss of data
Ensure that access rights to view and change data are managed effectively
Ensure that unusual data flows and system actions are monitored and quickly dealt with
Ensure that maintenance system administrators have received cybersecurity training
"Configuration Management Systems" (whether manual or automated) are required for PLCs, DCSs, HMIs, Industrial Networks, field instruments and process analyzers
Asset Management Systems must maintain adequate data to allow scanning for published CISA cybersecurity vulnerabilities.



This diagram shows maintenance activities as one of 4 Classes. The workflows and data involved with each of these may be quite different, so each is discussed separately below.

The workflows are indicated from intensive activities at the top, to less intensive activities at the bottom.

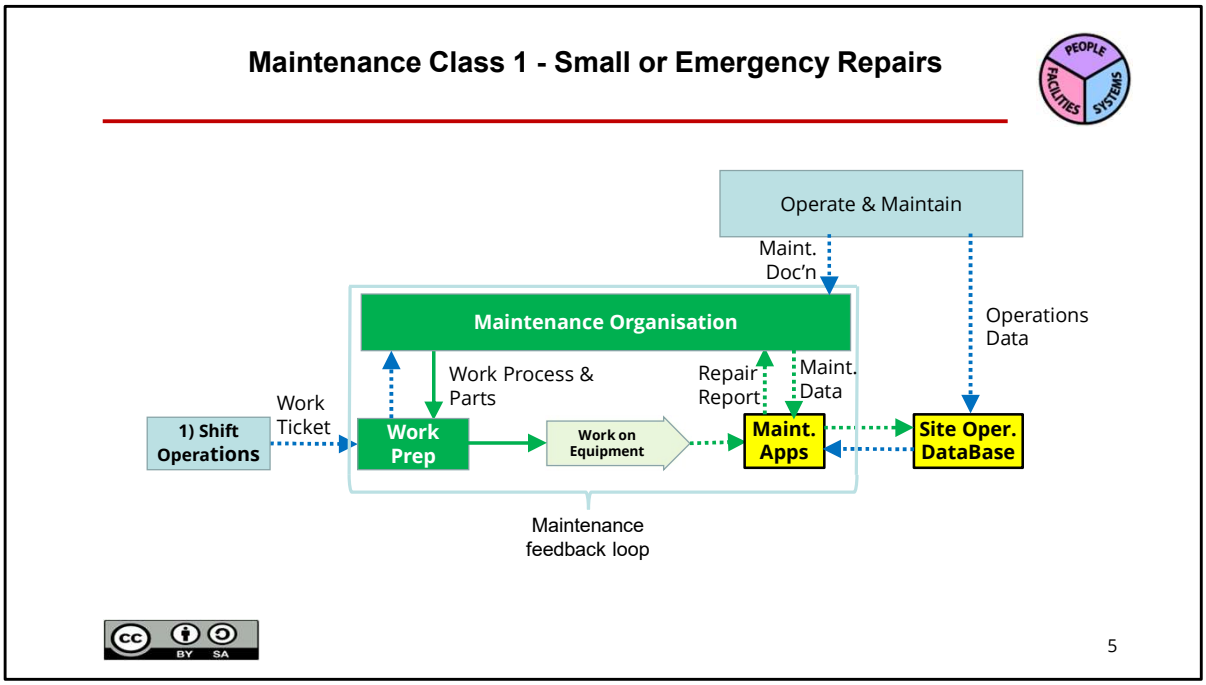
The following describes common aspects of these activities.

1) Small or emergency repairs - the Operations crew on shift will write a "ticket" to fix Controls or Instruments. The instrument technician on duty accepts the ticket and checks if he or she can repair it (without direction from the maintenance organization).

2) 2) Large repairs requiring parts and special skills (e.g. specialized resources and/or equipment, other discipline skills, or 3d-party support).

3) 3) Repairs requiring unit shutdown – Repairs or changes that require a Unit shutdown to be completed safely.

4) 4) Maintenance or Upgrades during scheduled Plant Turn-around - including those that require too much time or resources to be accomplished during normal plant operation.



1 - Small or emergency repairs - the Operations crew on shift will write a "Work Ticket" to fix Controls or Instruments. The instrument technician on duty accepts the ticket and checks if he or she can repair it (without direction or support from the maintenance organization).

After completion, a maintenance Repair Report is submitted referencing the instrument or device "Tag". The Maintenance Management System (or MMS) tracks work on that "Tag" so recurring or suspicious problems can be flagged for further investigation. Checking these records may identify recurring anomalies that may indicate a cybersecurity breach.

ACS software "patching" and/or intelligent device configuration changes are treated as small repairs. As with other repairs, an assessment of cyber risk if the patch is not accomplished forms part of the decision of whether to apply the patch immediately or wait for a shutdown.

In both small repairs and patching, the Repair Report should include updating the "Golden Copy" of the latest programs or equipment configuration. This is essential if future unapproved or malicious code changes are to be effectively detected.

Cybersecurity Checklist for Small or Emergency Repairs

	TASK
✓	Verify that electronic replacement parts and software updates have been procured with approved cybersecure procedures
✓	Verify that instrument and other device configuration devices (e.g. hand-held programmers) have been controlled to avoid viruses and changes
✓	Verify all data transfer devices (e.g. thumb drives or other media) have been scanned and those from vendors are certified.
✓	Affirm that technicians involved in maintenance have received cybersecurity training
✓	Consider whether the reported failures might have been caused by a cyber attack.
✓	Verify that the "Golden copy" of programs and configurations match what is currently installed.
✓	If repairs involve any program or configuration changes, make a new "Golden copy" and store this in the secure repository.

6

Verify that electronic replacement parts and software updates have been procured with approved cybersecure procedures

Verify that instrument and other device configuration devices (e.g. hand-held programmers) have been controlled to avoid viruses and changes

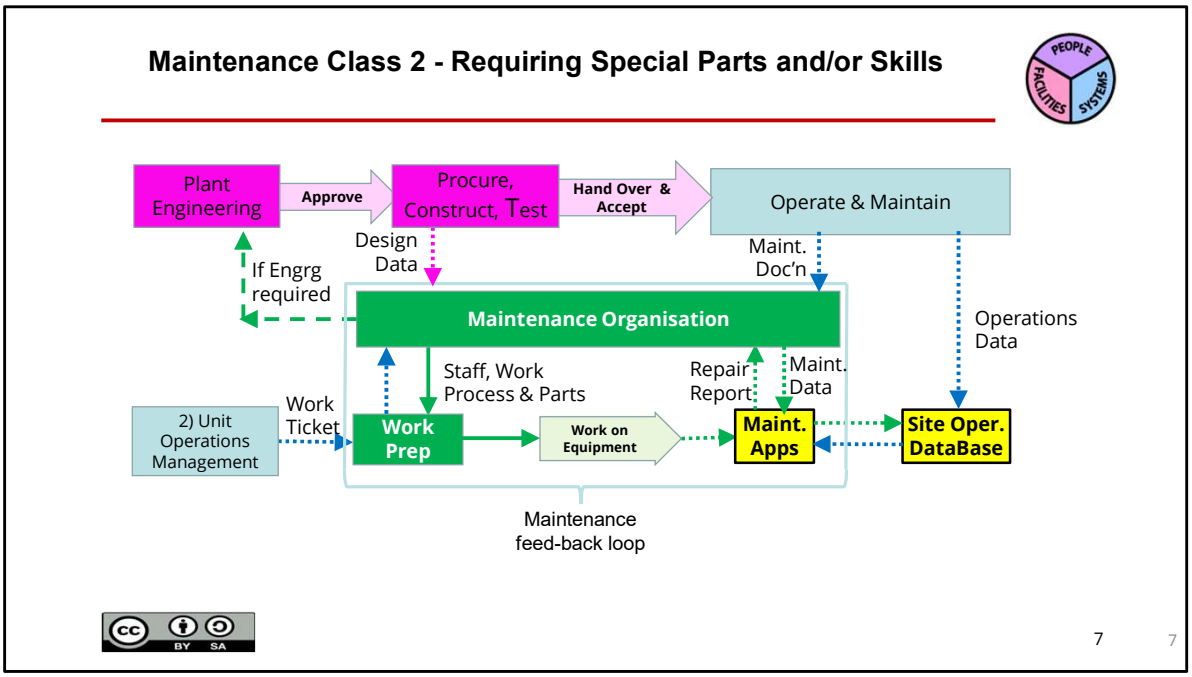
Verify that all data transfer devices (e.g., thumb drives or other media) have been scanned and that those from vendors are certified.

Affirm that technicians involved in maintenance have received cybersecurity training

Consider whether a cyber attack might have caused the reported failures.

Verify that the "Golden copy" of programs and configurations match what is currently installed.

If repairs involve any program or configuration changes, make a new "Golden copy" and store this in the secure repository.



2 - Repairs requiring special parts and/or skills – such as specialized resources and/or equipment, other discipline skills, or 3d party support).

A Work Order signed by Unit Operations Management is needed to take action. Plant Engineering, and/or Purchasing support may be required, if work is outside the capability of the Instrument maintenance department

A Maintenance Report is submitted referencing the equipment tags, parts, extra disciplines, engineering and/or other resources used. Data included should include any design information, test data, and initial production data. A new Golden Copy is stored of any new device configuration and/or programs.

Cybersecurity Checklist for Maintenance Requiring Special Parts or Skills

	TASK
✓	Verify that any specialist resources (from plant or a vendor) have received appropriate cybersecurity training.
✓	Verify that any published cyber vulnerabilities for instruments and control systems (typically from CISA) have been addressed.
✓	After programming and configuration changes are tested, verify that the new version of these are backed up (typically to a "Golden repository").
✓	Review data and/or code changes for cybersecurity vulnerabilities. Note: this might be done as part of "digital twin or other testing"
✓	Verify that parts drawn from maintenance stores have certified supply chains all the way back to the supplier.
✓	If remote access (e.g. for specialist support) is necessary, verify that approved procedures are followed to avoid introducing vulnerabilities.

CC BY SA

Verify that any specialist resources (from plant or a vendor) have received appropriate cybersecurity training.

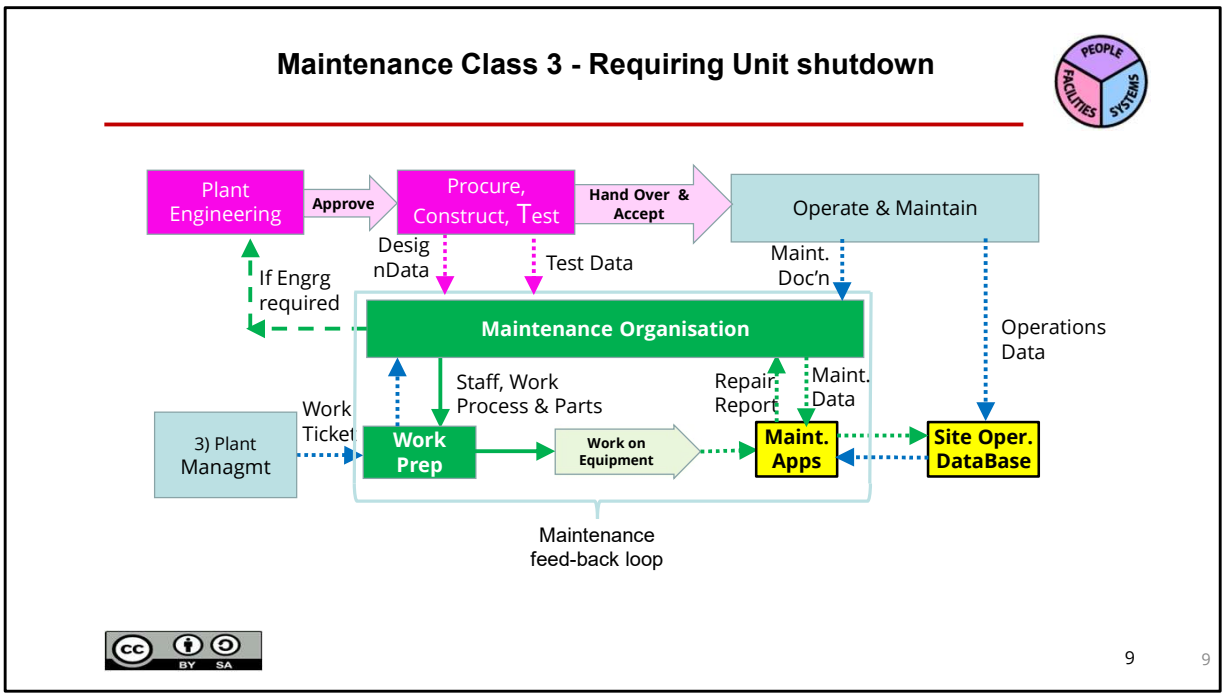
Verify that any published cyber vulnerabilities for instruments and control systems have been addressed.

After repairs are tested, verify that any data or code changes are backed up.

Review data and/or code changes for cybersecurity vulnerabilities. Note: this might be done as part of "digital twin or other testing."

Verify that parts drawn from maintenance stores have certified supply chains all the way back to the supplier.

If remote access (e.g. for specialist support) is necessary, verify that approved procedures are followed to avoid introducing vulnerabilities.



3) Maintenance requiring unit shutdown – Repairs or changes that require a Unit shutdown to be completed safely. This also includes non-urgent repairs where replacement can be delayed until the next shutdown when the work can be done more conveniently.

A work order signed by Plant Management is needed to take action.

The maintenance organization typically provides scheduling and supervision from plant shutdown to plant startup. External contractors or vendor support may be needed, requiring Plant Engineering, Procurement,

Certain equipment may need inspection and/or testing before approval to restart the production unit. A maintenance report is submitted referencing equipment tags, parts, extra disciplines, resources, and any test data.

Cybersecurity Checklist for Maintenance Requiring Unit Shutdown

	TASK
✓	Before shutdown, consider whether obsolete devices that cannot achieve the required Security Level may be replaced during shutdown.
✓	If appropriate, order replacements for any parts that cannot achieve the required Security Level for installation during the next shutdown.
✓	Verify that all purchase orders for replacement parts include the latest "cybersecurity requirements" as part of the purchase specification
✓	Review cybersecurity safety requirements in conjunction with process safety requirements for unit shutdown, startup testing, and operations.
✓	Conduct a cybersecurity check (according to plant procedures) to verify that vulnerabilities have not been introduced.

10

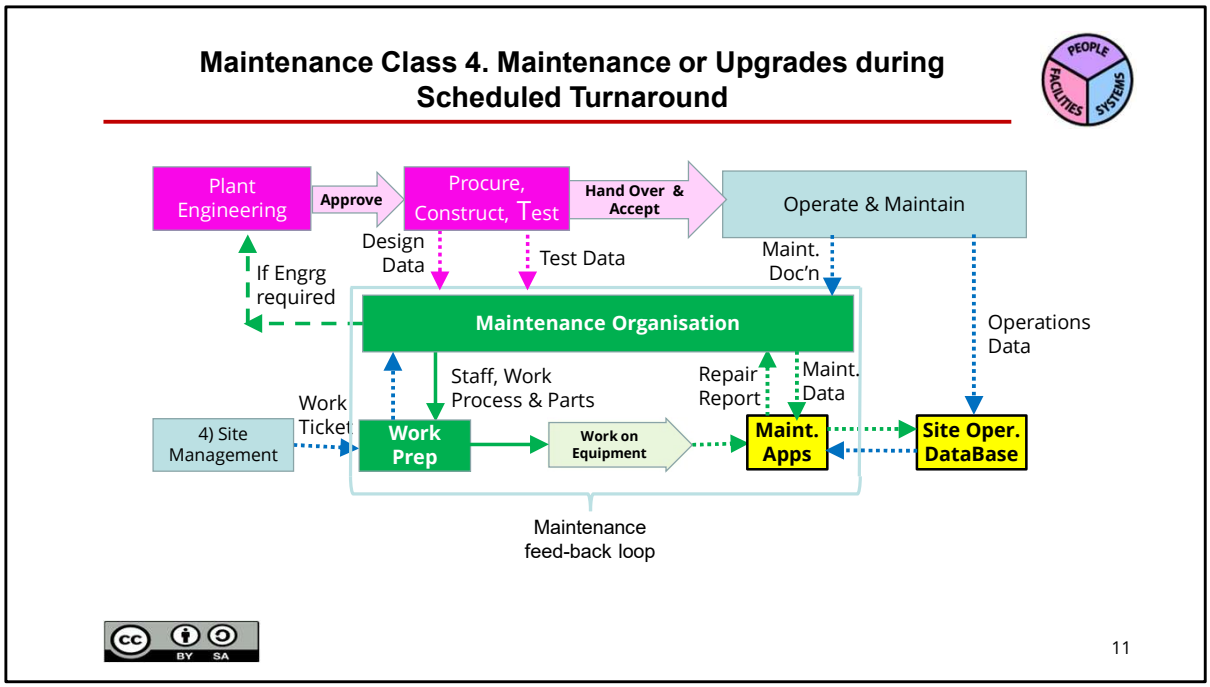
Before shutdown, consider whether obsolete devices that cannot achieve the required Security Level may be replaced during the shutdown.

If appropriate, order replacement parts that cannot achieve the required Security Level for installation during the next shutdown.

Verify that all purchase orders for replacement parts include the latest "cybersecurity requirements" as part of the purchase specification

Review cybersecurity safety requirements in conjunction with process safety requirements for unit shutdown, startup testing, and operations.

Conduct a cybersecurity check (according to plant procedures) to verify that vulnerabilities have not been introduced.



4. Maintenance or Upgrades during scheduled Plant Turnaround

This includes maintenance or upgrades that require too much time, resources or expertise to be safely accomplished during normal plant operations. This typically involves external contracts, Plant Engineering, Procurement and Construction support.
A Plant Turnaround Report and/or a Project Report is submitted referencing equipment tags, reports from all disciplines involved, and/or resources consumed. Data captured should include any design information, test data, and initial production data, as well as a Golden Copy of any new device configuration and/or programs.

Information (data) is derived from the Site Operations Database and the Maintenance organization. This diagram shows the maintenance loop, the sequence of activities. This is a work order based loop (system). The work is to be prepared by workpreparation as organisation (spare parts, scafolding, hoisting equipment) may be required.

Cybersecurity Checklist for Major Turnarounds or Upgrades

	TASK
✓	Before Plant Turnaround, verify that all contracts for maintenance or unit upgrades contain the appropriate cybersecurity clauses.
✓	All new instrumentation, PLCs, HMIs, and industrial networks, etc., should be reviewed for cyber vulnerabilities.
✓	Inform the maintenance data system administrator of the Security Level of any new ACS being added or upgraded.
✓	Ensure that data access provisions are made in the maintenance data management system (including user accounts with minimum required access)
✓	Ensure that data recovery is tested for “simulated cybersecurity attack”

CC BY SA

12

This Cybersecurity checklist for a Major Turnaround or Upgrade should include all relevant items from the checklist for each of the previous workflows.

Well before the plant turnaround begins, verify that all contracts for maintenance or unit upgrades contain the appropriate cybersecurity clauses.

All new instrumentation, PLCs, HMIs, and industrial networks, etc., should be reviewed for cyber vulnerabilities.

Inform the maintenance data system administrator of the Security Level of any new ACS being added or upgraded.

Ensure that all necessary data access provisions are made in the maintenance data management system (including user accounts with minimum required access)

Ensure that data recovery is tested for “simulated cybersecurity attack”

Example Cybersecurity Checklist

Checklist Process Control Apparatus: Control valve / on-off valve	Form 33				Project No..... Doc. No. .....
Maintenance Type	Activity	Checked			Remarks
		Yes	No	N.A.	
1 Emergency Maintenance	• Verify that electronic replacement parts and software updates have been procured with approved cybersecure procedures • Verify that instrument and other device configuration devices (e.g. hand-held programmers) have been controlled to avoid viruses and changes • Verify that all data transfer devices (e.g., thumb drives or other media) have been scanned and that those from vendors are certified. • Affirm that technicians involved in maintenance have received cybersecurity training • Consider whether a cyber attack might have caused the reported failures. • Verify that the "Golden copy" of programs and configurations match what is currently installed. • If repairs involve any program or configuration changes, make a new "Golden copy" and store this in the secure repository.				See inspection
2 Requiring Special Parts or Experience	• Verify that electronic replacement parts and software updates have been procured with approved cybersecure procedures • Verify that instrument and other device configuration devices (e.g. hand-held programmers) have been controlled to avoid viruses and changes • Verify that all data transfer devices (e.g., thumb drives or other media) have been scanned and that those from vendors are certified. • Affirm that technicians involved in maintenance have received cybersecurity training • Consider whether a cyber attack might have caused the reported failures. • Verify that the "Golden copy" of programs and configurations match what is currently installed. • If repairs involve any program or configuration changes, make a new "Golden copy" and store this in the secure repositor				See inspection

CC BY SA

13

This sheet is an example Checklist format that may be used for manual or electronic data records.

Key Messages

The following are key messages to take away:

- **Terminology:**
  - Golden copy – a secured version of PLC or RTU programs and configuration
  - Configuration Management Software – manage control device and network programs and configuration
  - CISA – US Cybersecurity Infrastructure and Security Agency
- **What is Needed:**
  - Cybersecurity training for all staff
  - Approved cybersecure procedures for engineering, maintenance, and procurement

The following are key messages to take away:

Terminology:
Golden copy – the latest version of a PLC or RTU program or device or network configuration
Configuration Management Software – manages control device and network programs and configuration
CISA – US Cybersecurity Infrastructure and Security Agency

What is Needed:
Cybersecurity training for all staff
Approved cybersecure procedures for engineering, maintenance, and procurement.

Further Information

- **Related MLMs**
  - MLM-035-A Secure PLC and RTU Concepts
  - MLM-035-B Secure PLC and RTU Programming
  - MLM-035-C Secure PLC and RTU Operations
  - MLM-035-D Secure PLC and RTU Mods and Upgrades
  - MLM-035-E Secure PLC and RTU AI Validation & Programming
  - MLM-078-A Intelligent Device Configuration

Please click here to send us your feedback.

https://creativecommons.org/licenses/by-sa/4.0/

Here are some web links to related MLMs

Please use this link to share your comments. These will be shared with the author to help improve future versions.

Author

Hindrik Koning

Hindrik is a Senior Engineer with deep knowledge of data exchange and sharing in plant environments.

CC BY SA