E

Eolas Automation

AUTOMATION RESILIENCE AND RECOVERY SURVEY

# Plant Controls Resilience Survey Sample Report

Fictional Midlands Packaging Plant | Production Line 2

## How prepared is the site for a controls failure?

An evidence-based assessment of installed controls, network architecture, software recovery, drawing accuracy, lifecycle exposure and single points of failure.

ILLUSTRATIVE SAMPLE

All site names, assets and findings in this report are fictional.

Prepared to demonstrate the Eolas Automation survey format and engineering approach.

EXECUTIVE SUMMARY

# Recovery readiness is not yet fully evidenced

The sample assessment found a functioning controls estate with several gaps affecting recovery confidence. The main findings relate to incomplete backup verification, undocumented network dependencies, ageing drives and drawings that do not fully match the installed plant. If one of the identified control points failed, the missing information may extend diagnosis and restoration time.

| 4 | 1 | 1 | 0 |
|---|---|---|---|
| PRIORITY FINDINGS | CRITICAL DRIVE WITHOUT SPARE | UNMANAGED LINE SWITCH | NETWORK DRAWINGS AVAILABLE |

## Engineering conclusion

The current recovery position relies partly on undocumented knowledge and ageing assets. A practical follow-up would be to verify backups, drawings and network information, then review the main conveyor drive application. Any replacement programme could then be phased using operational criticality, available spares and recovery confidence rather than age alone.

## Priority findings

- The main line PLC has a stored project file, but the current online version has not been verified against that source.
- One unmanaged line switch and an undocumented PLC-to-PLC data path create potential single points of failure.
- The main conveyor Micromaster drive has no tested replacement plan and its parameter set is not included in the site recovery pack.
- Electrical drawings reflect the original installation but omit later remote I/O, safety and network changes.

SURVEY SCOPE

# What the survey examines

The survey is designed for maintenance and engineering teams. It combines a physical walkdown, structured interviews, document review and non-intrusive checks. No live control changes are made unless separately agreed.

| Area | Included review | Site question |
|---|---|---|
| Installed base | PLCs, HMIs, drives, safety, remote I/O, switches and gateways | What is installed and which assets are critical? |
| Recovery | Project files, drive parameters, versions, licences and restore requirements | Could the site rebuild after a failed device? |
| Architecture | Control boundaries, data exchange, networks and single points of failure | Where could one failure stop several machines? |
| Documentation | Electrical drawings, network diagrams, asset lists and revision control | Do records match the plant? |
| Lifecycle | Support status, spares, lead times and migration paths | What may need attention first and why? |
| Roadmap | Immediate controls, planned work and budget bands | What decisions are needed now, next year and later? |

## Assessment scale

| Rating | Meaning | Suggested follow-up |
|---|---|---|
| Critical | Recovery is not reasonably assured and production exposure is immediate. | Review promptly and agree interim controls. |
| High | A failure may lead to material or extended downtime. | Consider action within the near-term work plan. |
| Medium | The weakness is manageable but affects resilience. | Include in planned maintenance or improvement work. |
| Low | Controls appear adequate with routine maintenance required. | Retain under periodic review. |

## Sample survey basis

Illustrative scope: one production line, 17 control assets, six drives, four PLCs, two HMIs, one safety controller, four network devices and associated electrical documentation. The sample assumes a two-day site visit followed by engineering review and report preparation.

PRIORITY FINDINGS

# Findings that may contribute to extended downtime

| ID | Finding | Rating | Evidence | Suggested follow-up |
|---|---|---|---|---|
| R01 | Unverified PLC source | High | Stored project date predates the last modification. | Online comparison during an agreed window and archive of verified source. |
| R02 | Micromaster failure | High | Critical conveyor; no commissioned spare or migration pack. | Parameter capture and review of a possible G120 replacement design. |
| R03 | Network single point | High | One unmanaged switch connects PLC, HMI and remote I/O. | Topology documentation and assessment of a managed industrial switch. |
| R04 | Drawing inaccuracy | High | Remote I/O and safety changes absent from drawings. | Red-line walkdown and controlled as-built drawing update. |
| R05 | Engineering laptop dependency | Medium | Required software versions exist on one laptop only. | Toolchain and licence record with a review of recovery-machine options. |
| R06 | PLC proliferation | Medium | Two add-on PLCs exchange permissives through undocumented signals. | Dependency mapping and possible consolidation during a future upgrade. |
| R07 | HMI image not tested | Medium | Backup present but restore method and runtime licence unconfirmed. | Restore instruction and validation against suitable spare hardware. |

## Basis for ratings

The ratings express an engineering judgement for this fictional example, based on production impact, spare availability, backup status and the information needed to restore each system. They are not a measured probability of failure or a numerical condition score.

CONTROLS ARCHITECTURE

# Small additions have created hidden dependencies

The original line controller remains the main production authority, but later additions introduced separate PLCs and unmanaged network paths. The machinery may appear independent while still depending on shared permissives and one switch.

| | | |
|---|---|---|
| **LINE PLC**<br>**S7-1500 · main sequence** | | **HMI**<br>**Operator control** |
| ↓ PROFINET | | ↑ |
| **UNMANAGED SWITCH 01**<br>**Single point of failure** | **REMOTE I/O**<br>**ET200 station** | **SAFETY PLC**<br>**Interlocks and muting** |
| ↓ | | ↓ undocumented permissive |
| **DRIVE GROUP**<br>**Micromaster and G120** | **ADD-ON PLC A**<br>**Retrofit subsystem** | **ADD-ON PLC B**<br>**Packaging interface** |

## Architecture observations

■ The line topology has no controlled network drawing and device addresses are maintained informally.

■ Add-on PLCs expanded functionality but also added interfaces that are not visible in the main sequence documentation.

■ A managed switch and documented port map would improve fault diagnosis and create evidence for future segmentation.

■ A suitable end state would favour clear ownership, documented dependencies and recoverable configurations rather than consolidation for its own sake.

RECOVERY AND DOCUMENTATION

# A backup only has value when the site can identify and restore it

| System | Backup | Verified current | Restore method | Status |
|---|---|---|---|---|
| Line PLC | Available | No | Partial instruction | High |
| Safety PLC | Available | Yes | Engineer dependent | Medium |
| Main HMI | Image available | No | Licence unclear | High |
| G120 drive group | Parameter files | Yes | STARTDRIVE project | Low |
| Micromaster conveyor | Paper list only | No | No tested method | High |
| Add-on PLC A | Available | Unknown | Software version recorded | Medium |

## Drawing accuracy sample

| Drawing set | Latest revision | Field match | Finding |
|---|---|---|---|
| Main power | 2022 | 85% | Generally accurate; two drive substitutions not revised. |
| Control circuits | 2019 | 55% | Later sensors and remote I/O changes missing. |
| Safety circuits | 2018 | 40% | Interlock and muting changes not incorporated. |
| Network architecture | Not available | 0% | Topology could be created from the site survey. |

## Suggested recovery pack

- Verified project and parameter files with date, device, software version and responsible reviewer.
- Plain-language restoration instructions, required cables, licences and replacement hardware notes.
- Current electrical drawings, network topology, IP schedule and controlled change log.
- Quarterly backup register review and an annual sample restore exercise.

LIFECYCLE AND SPARES

# Replacement priority can follow production consequence

Age is useful evidence but not the decision on its own. Priority can consider lifecycle status, operational criticality, spares, recovery confidence and the time required to engineer a safe replacement.

| Asset | Lifecycle position | Site spare | Production impact | Possible follow-up |
|---|---|---|---|---|
| Micromaster conveyor drive | Obsolete | No | Line stopped | Review of a possible G120 migration pack |
| S7-300 utility PLC | Mature / limited | Used spare | Reduced production | Backup verification and possible S7-1500 migration plan |
| Legacy HMI panel | Obsolete | No | Manual recovery difficult | Replacement HMI project assessment |
| G120 drive group | Supported | One | Area stopped | Parameter archive and spare-strategy review |
| S7-1500 line PLC | Supported | No | Line stopped | Delivery route and recovery-image confirmation |

## Drive migration planning

For the Micromaster application, the survey can capture more than the drive nameplate. A migration pack may record motor data, braking arrangement, fieldbus or hardwired interface, safety requirements, speed references, feedback devices, cabinet space, heat, protection, cable requirements, operating sequence and acceptance criteria. This gives the site better information for pricing and scheduling a possible G120 replacement.

## Indicative migration option comparison

| Option | Downtime exposure | Engineering confidence | Observation |
|---|---|---|---|
| Wait for failure | Unknown and potentially prolonged | Low | Higher uncertainty |
| Hold uncommissioned spare | Reduced hardware delay only | Medium | Interim risk control |
| Engineer and test migration | Planned and bounded | High | Lower uncertainty |

SUGGESTED ROADMAP

# A practical sequence for follow-up work

The suggested roadmap separates straightforward verification work from planned engineering changes. Budget bands are illustrative and would be confirmed only after scope definition and supplier pricing.

| Timing | Work package | Outcome | Budget band |
|---|---|---|---|
| 0-30 days | Critical PLC, HMI and drive backup verification; controlled recovery register | Known current source and accountable ownership | Low |
| 0-90 days | Network topology and IP schedule; assessment of the main-line unmanaged switch | Faster diagnosis and reduced single-point exposure | Low to medium |
| 0-90 days | Red-line review of priority electrical and safety drawings | Accurate maintenance information for priority systems | Medium |
| 3-6 months | Micromaster to G120 migration design and pre-commissioning review | Bounded shutdown and tested recovery route | Medium |
| 6-12 months | Legacy HMI replacement assessment and validated restore pack | Supported operator interface with recoverable project | Medium |
| 1-3 years | Review of add-on PLC interfaces during a planned machine upgrade | Simpler architecture and fewer hidden dependencies | Capital project |

## Suggested next step

A suitable starting point would be the backup verification, network documentation and drawing review listed in the first 90 days. The conveyor drive migration could then be assessed in more detail. Wider controller consolidation may be considered during a future planned line upgrade once the present interfaces are documented.

## Periodic review

The controls resilience position may be reviewed annually or after significant plant changes. A follow-up review can confirm whether critical backups remain current, drawings reflect completed changes, new network devices are documented and earlier findings remain relevant.

SAMPLE ASSET REGISTER

# Installed base evidence behind the decisions

| Tag | Asset | Platform | Software / interface | Backup | Risk |
|---|---|---|---|---|---|
| PLC-L2-01 | Main line controller | Siemens S7-1515F | TIA Portal V18 / Profinet | Present, unverified | High |
| PLC-L2-02 | Utility controller | Siemens S7-315 | Step 7 V5.6 / Profibus | Verified 2024 | Medium |
| PLC-L2-03 | Retrofit controller | Schneider M340 | Ethernet data exchange | Present | Medium |
| HMI-L2-01 | Main operator panel | Legacy 15 inch panel | WinCC runtime | Image unverified | High |
| DRV-L2-01 | Main conveyor | Micromaster | Hardwired I/O | Paper parameters | High |
| DRV-L2-02 | Feed conveyor | Siemens G120 | Profinet / STO | Verified | Low |
| NET-L2-01 | Line switch | Unmanaged industrial | No diagnostics | No configuration | High |
| RIO-L2-01 | Remote I/O | ET200SP | Profinet / Profisafe | Within PLC project | Low |

## Register ownership

The final survey register would include manufacturer, model, serial number, firmware, network address, cabinet location, process function, criticality, spare status, lifecycle position, backup reference, drawing reference, photo reference and suggested follow-up. The customer retains a usable register rather than a report that becomes static on the day of issue.

FOLLOW-UP SUMMARY

# Suggested follow-up for the site team

This page summarises the engineering findings and possible next steps for internal review.

| Suggested follow-up | Basis | Possible lead | Indicative timing |
|---|---|---|---|
| Verify critical backups | Current source cannot be proven for all priority systems | Engineering | Near term |
| Document the network and review the main switch | One device failure may affect the full line | Maintenance | Near term |
| Assess Micromaster to G120 migration | Obsolete critical drive with no tested replacement route | Engineering | Planned review |
| Update priority drawings | Safety and remote I/O changes are absent from the current set | Engineering | Planned review |
| Revisit resilience after plant changes | Plant changes continually alter the recovery position | Site team | Periodic |

## What Eolas Automation would deliver

- A concise executive overview suitable for internal review and capital planning.
- A detailed multi-vendor controls asset register with evidence and photographs.
- A network and control architecture drawing that reflects the installed plant.
- A backup, drawing and recovery register showing what is verified and what is missing.
- A prioritised action plan with immediate controls, planned upgrades and budget bands.

## About this sample

This document demonstrates the proposed Eolas Automation report format. All site information and findings are fictional. A real survey would be based on agreed scope, site access, production constraints and evidence gathered during the assessment.

**Eolas Automation**
Industrial automation support, resilience surveys, fault finding and practical upgrades for existing production sites.
Portlaoise, County Laois | eolasautomation.com