OT CRUCIBLE

AFTER-ACTION REPORT / IMPROVEMENT PLAN

# BLACK FORGE — Sample Exercise

## OTC-MFG-001 · BLACK FORGE — RANSOMWARE MEETS THE FACTORY

ORGANIZATION
Meridian Precision Systems (fictional)

DATE
August 24, 2026

FACILITY
Meridian Precision Systems — Plant 1

FORMAT / DURATION
STANDARD · 90 minutes

## 1. Executive summary

| 1 | 2 | 1 | 1 | 0 | 1 | 1 |
|---|---|---|---|---|---|---|
| PARTICIPANTS | INJECTS | DECISIONS | OBSERVATIONS | STRENGTHS | IMPROVEMENTS | ACTIONS |

The scenario: A precision manufacturer begins experiencing enterprise system disruption consistent with a ransomware event. Engineering and production data systems become partially unavailable, and the team must decide what to isolate, whether production can continue, whether manufacturing data can be trusted, how customer commitments are handled, and what a trustworthy return to production requires.

BLACK FORGE is grounded in documented real-world events, including: 2019 ransomware at Norsk Hydro forced manual plant operations across 170 sites worldwide; CISA #StopRansomware advisories document ransomware repeatedly reaching manufacturing OT. The exercise asks the team to face the same pressures with their own facility, people, and commitments.

Meridian Precision Systems (Demo) conducted BLACK FORGE (OTC-MFG-001), a facilitated 90-minute standard exercise at Meridian Precision Systems — Plant 1. 1 participant worked through 2 injects, recording 1 decision while evaluators captured 1 observation.

What the team got right: "Declare an incident and name an incident commander" (Evidence quality +5, Team coordination +15). Consequence values are the scenario's authored, deterministic effects — the same choices always score the same way.

1 area was identified for improvement, including: OT not represented in initial incident command. 1 corrective action has been defined with owners and target dates tracked in the improvement plan.

Results reflect performance observed during this exercise only. They do not constitute certification, compliance determination, or a measure of overall security posture.

## 2. Exercise overview

| | |
|---|---|
| Organization | Meridian Precision Systems (fictional) |
| Facility | Meridian Precision Systems — Plant 1 |
| Scenario | OTC-MFG-001 BLACK FORGE |
| Format | STANDARD · 90 minutes |
| Conducted | 8/24/2026, 6:29:12 PM |
| Participants | Pat Operator (IT Director / Security Lead) |

## 3. Exercise objectives

OBJ-01 **Incident authority** — Determine whether authority and responsibility for industrial cyber incident response are clearly understood.

OBJ-02 **Detection and validation** — Evaluate how the organization validates suspected cyber effects affecting operations.

OBJ-04 **IT/OT coordination** — Assess coordination among IT, OT, operations, engineering, quality, and safety functions.

OBJ-05 **Containment** — Assess decision-making surrounding isolation or containment while accounting for operational consequences.

OBJ-06 **Product & service integrity** — Determine how the organization establishes confidence in operational data and the integrity of its product or service.

OBJ-08 **Customer response** — Evaluate how customer commitments and product-assurance questions are handled.

OBJ-10 **Recovery prioritization** — Determine whether restoration priorities align with critical production dependencies.

OBJ-11 **Known-good restoration** — Evaluate how the organization establishes a trustworthy baseline prior to restarting production.

OBJ-12 **Backup validation** — Evaluate whether required systems, configurations, and production data can actually be restored.

## 4. Scenario background

A precision manufacturer begins experiencing enterprise system disruption consistent with a ransomware event. Engineering and production data systems become partially unavailable, and the team must decide what to isolate, whether production can continue, whether manufacturing data can be trusted, how customer commitments are handled, and what a trustworthy return to production requires.

**The setting:** A discrete precision manufacturer operating two shifts. Production depends on digital manufacturing data flowing from an engineering repository through a distribution system to CNC, robotic, and additive cells, with quality verification recorded in a quality database. It is 08:00 on a normal Tuesday; a priority customer shipment is scheduled for 15:00.

### Where the exercise begins

• All production cells are running scheduled jobs.

• Enterprise identity, email, ERP, engineering repository, and scheduling are operating normally at exercise start.

• The backup platform reports green status on its dashboard.

• A machine-tool vendor holds a remote-support connection used for one robotic cell.

### Grounded in real events

**2019 ransomware at Norsk Hydro forced manual plant operations across 170 sites worldwide (2019-03-19).** BLACK FORGE's central arc — enterprise systems failing while production keeps moving, and the discipline of a trustworthy return to production — mirrors how Hydro ran plants manually rather than pay.

**CISA #StopRansomware advisories document ransomware repeatedly reaching manufacturing OT.** The scenario's decision points follow the advisories' recurring themes: segmentation choices under pressure, data-integrity doubt, customer communications discipline, and verified restoration.

M1 **Something Is Wrong** — Early indicators of enterprise disruption. The team must decide who is in command before anyone knows how bad it is.

M2 **The Factory Feels It** — Production can no longer reliably pull digital manufacturing data, and quality surfaces an integrity question. Availability and integrity stop being the same problem.

M3 **Containment Has a Price** — Every containment option costs production something. A customer asks the question nobody is ready for, and a vendor offers help through the pathway under suspicion.

M4 **Recovery Is the Hard Part** — Spread appears contained. Now the harder questions: what does 'restored' mean, in what order, and on what evidence does the factory restart?

## 5. Timeline

| | | |
|---|---|---|
| 06:29 PM | FACILITATOR | LAUNCH |
| 06:29 PM | INJECT | Engineering shares unreachable — STATUS UPDATE |
| 06:29 PM | INJECT | Security monitoring raises the alarm — DECISION POINT |
| 06:29 PM | DECISION | Pat Operator (IT Director / Security Lead) — Chose: Declare an incident and name an incident commander |
| 06:29 PM | RESOLUTION | Room decision: Security monitoring raises the alarm — Declare an incident and name an incident commander |
| 06:29 PM | FACILITATOR | END MODULE |
| 06:29 PM | FACILITATOR | END MODULE |
| 06:29 PM | FACILITATOR | END MODULE |
| 06:29 PM | FACILITATOR | END EXERCISE |

## 6. Key decisions

**Security monitoring raises the alarm**

Who takes command of the response right now, and what is the immediate priority?

ROOM DECISION: Declare an incident and name an incident commander

Pat Operator (IT Director / Security Lead): Declare an incident and name an incident commander

## 7. Decision assessment

The room's resolved decisions, scored by the scenario's authored, deterministic consequences. "What good looks like" is the scenario author's evaluation guidance for that moment.

**Security monitoring raises the alarm**

CHOSE: Declare an incident and name an incident commander

Evidence quality +5 · Team coordination +15

What good looks like: Time how long command takes to establish and whether authority is named or assumed. Note whether OT/production is included in the initial command structure (OBJ-01, OBJ-04).

## 8. Strengths

None were recorded.

## 9. Areas for improvement

**OT not represented in initial incident command**

MEDIUM CONFIDENCE · OBSERVED

During Inject 3 the incident commander was named quickly, but the response bridge did not include OT or production representation until later in the exercise.

## 10. Objective performance

Exercise Response Score — performance observed in this exercise only. Not a compliance or maturity measure.

| | | |
|---|---|---|
| OBJ-01 **Incident authority**<br>Incident command was established within four minutes of the alert. | **3 — Effective** |
| OBJ-02 **Detection and validation** | **Not assessed** |
| OBJ-04 **IT/OT coordination** | **Not assessed** |
| OBJ-05 **Containment** | **Not assessed** |
| OBJ-06 **Product & service integrity** | **Not assessed** |
| OBJ-08 **Customer response** | **Not assessed** |
| OBJ-10 **Recovery prioritization** | **Not assessed** |
| OBJ-11 **Known-good restoration** | **Not assessed** |
| OBJ-12 **Backup validation** | **Not assessed** |

## 11. Operational impact analysis

Simulated estimates from the deterministic exercise engine. Values reflect scenario-modeled consequences of the decisions made, not measured business impact.

| | | |
|---|---|---|
| Production availability | 100 » 100 | 0 |
| IT visibility | 90 » 85 | -5 |
| OT visibility | 85 » 85 | 0 |
| Product integrity confidence | 95 » 95 | 0 |
| Containment confidence | 40 » 35 | -5 |
| Recovery confidence | 60 » 60 | 0 |
| Safety margin | 90 » 90 | 0 |
| Customer confidence | 90 » 90 | 0 |
| Team coordination | 60 » 75 | +15 |
| Evidence quality | 50 » 55 | +5 |
| Financial impact | 0 » 0 | 0 |

## 12. Framework alignment

Framework references are provided for improvement planning only. They indicate that exercise observations are relevant to the cited guidance; they are not a compliance assessment or certification. Draft publications are labeled and must not be treated as final.

| | | |
|---|---|---|
| NIST | NIST CSWP 29 2.0 — The NIST Cybersecurity Framework (CSF) 2.0 | FINAL |
| NIST | IR 8374 Rev. 1 — Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile | FINAL |
| NIST NCCoE | SP 1800-41 — Responding to and Recovering from a Cyber Attack: Cybersecurity for the Manufacturing Sector | INITIAL PUBLIC DRAFT |

| | | |
|---|---|---|
| NIST | SP 800-61 Rev. 3 — Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile | FINAL |
| NIST | SP 800-82 Rev. 3 — Guide to Operational Technology (OT) Security | FINAL |

## 13. Corrective action plan

**Add OT representation to incident command activation checklist**

MEDIUM PRIORITY · OPEN · UNASSIGNED

FROM FINDING: OT not represented in initial incident command

## 14. What was not tested

### Injects not delivered

- ERP slows to a crawl
- Machines can't get their programs
- Revision discrepancy on a live job
- The rumor mill starts
- IT recommends isolation
- The customer asks the hard question
- The vendor offers a remote hand
- Contained — now what?
- The backup that wasn't
- Speed or evidence
- How do you know you're back?

### Objectives not assessed

- OBJ-02 — Detection and validation
- OBJ-04 — IT/OT coordination
- OBJ-05 — Containment
- OBJ-06 — Product & service integrity
- OBJ-08 — Customer response
- OBJ-10 — Recovery prioritization
- OBJ-11 — Known-good restoration
- OBJ-12 — Backup validation

### Out of scope by design

- Technical forensics and malware analysis technique
- Law-enforcement engagement specifics
- Ransom negotiation strategy
- Actual regulatory or contractual legal determinations

## 15. Appendix — how to read this report

An OT Crucible exercise is a facilitated tabletop: the facilitator publishes injects (scripted events) on a human tempo, participants respond in role, and decision points force the room to choose between authored options. Nothing in this report is generated text — every statement derives from what was recorded during the exercise.

Consequences are deterministic. Each decision option carries author-defined effects on the scenario's operational gauges (0–100 scales where higher is better). The same choices always produce the same scores, which is what makes results comparable across teams and across time.

Findings and objective ratings are human judgments recorded by evaluators, each carrying its confidence and provenance. Corrective actions are the exercise's lasting output: owned, dated, and tracked to closure — a later exercise validates that closure.

### Glossary

**Inject —** A scripted event delivered to participants during the exercise — an alert, a report, a request, or a decision point.

**Decision point —** An inject that requires the room to choose between authored options; the chosen option's effects are applied by the engine.

**Operational gauge —** A 0–100 scenario state variable (e.g. containment confidence, service availability). Higher is always better; 70+ reads healthy, 40–69 strained, below 40 critical.

**Role-private information —** Inject detail visible to one role only, so different seats experience the same moment differently — as in a real incident.

**Finding (strength / improvement) —** An evaluator-recorded conclusion tied to evidence from the exercise, with stated confidence and provenance.

**Exercise Response Score —** The 0–4 rubric applied per objective: Not demonstrated, Limited, Partial, Effective, Strong. It measures this exercise only.

**Corrective action —** A tracked improvement commitment with an owner, priority, and target date, derived from a finding.

**Hotwash —** The facilitated debrief immediately after the last inject, while impressions are fresh.

## 16. Appendix — participant feedback

**What worked well?**

Pat Operator: "Command was established fast and roles were clear."

## 17. Appendix — source registry

| | | |
|---|---|---|
| Aviation Information Sharing and Analysis Center | Aviation ISAC (A-ISAC) | REFERENCE ONLY |
| American Petroleum Institute (API) | API Standard 1164 — Pipeline Control Systems Cybersecurity | REFERENCE ONLY |
| ASHRAE / BACnet International | ANSI/ASHRAE 135 — ANSI/ASHRAE Standard 135 (BACnet) & BACnet Secure Connect (BACnet/SC) | REFERENCE ONLY |
| American Water Works Association (AWWA) | Water Sector Cybersecurity Risk Management Guidance & Assessment Tool | REFERENCE ONLY |
| BIMCO / International Chamber of Shipping (ICS) | Guidelines on Cyber Security Onboard Ships | REFERENCE ONLY |
| CCSDS | CCSDS 355.0-B — Space Data Link Security Protocol (CCSDS 355.0-B) | REFERENCE ONLY |
| CISA | AA20-049A — Ransomware Impacting Pipeline Operations | FINAL |
| CISA/DOE/NSA/FBI | AA22-103A — APT Cyber Tools Targeting ICS/SCADA Devices (PIPEDREAM/INCONTROLLER) | FINAL |
| CISA + partners | AA23-335A — IRGC-Affiliated Cyber Actors Exploit Unitronics PLCs in the Water and Wastewater Sector | FINAL |
| CISA/NSA/FBI | AA24-038A — PRC State-Sponsored Actors (Volt Typhoon) Compromise and Maintain Persistent Access to US Critical Infrastructure | FINAL |
| CISA/FBI/NSA/EPA | AA26-097A — Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure | FINAL |
| CISA | Chemical Facility Anti-Terrorism Standards (CFATS) & Chemical Sector resources | REFERENCE ONLY |
| CISA | Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022) — reporting requirements | REFERENCE ONLY |
| CISA | Cross-Sector Cybersecurity Performance Goals | FINAL |

| | | |
|---|---|---|
| CISA (US DHS) | Critical Manufacturing Sector (incl. Primary Metal Manufacturing) | REFERENCE ONLY |
| CISA | CISA Tabletop Exercise Packages (CTEP) | REFERENCE ONLY |
| CISA / USDA / FDA | Food and Agriculture Sector — Critical Infrastructure Security & Resilience | REFERENCE ONLY |
| CISA | CISA ICS Advisories (Building Automation & Data-Centre Products) | REFERENCE ONLY |
| CISA | ICS Advisory ICSA-25-191-10 — End-of-Train / Head-of-Train Remote Linking (CVE-2025-1727) | FINAL |
| CISA / TSA / DOT | Transportation Systems Sector (SRMA guidance) | REFERENCE ONLY |
| CENELEC / IEC | CLC/TS 50701 and (forthcoming) IEC 63452 — Railway applications cybersecurity | REFERENCE ONLY |
| US Department of Energy | DOE Form OE-417 — Electric Emergency Incident and Disturbance Report | FINAL |
| European Union Aviation Safety Agency (EASA) | EASA Part-IS — Information Security (Reg (EU) 2023/203 & Delegated Reg (EU) 2022/1645) | REFERENCE ONLY |
| ENISA | ENISA — Railway Cybersecurity guidance | REFERENCE ONLY |
| US EPA | America's Water Infrastructure Act §2013 / Safe Drinking Water Act §1433 — Risk & Resilience Assessments and Emergency Response Plans | FINAL |
| US EPA | Risk Management Program (RMP) — Clean Air Act §112(r) / 40 CFR 68 | FINAL |
| US EPA | Oil Pollution Prevention — Spill Prevention, Control, and Countermeasure (SPCC, 40 CFR 112) and NCP reporting | FINAL |
| European Commission / EMA | EU GMP Annex 11 — Computerised Systems (EudraLex Vol. 4) | REFERENCE ONLY |
| European Union / ENISA | NIS2 Directive (EU 2022/2555) | REFERENCE ONLY |
| US Federal Aviation Administration | FAA — National Airspace System, NOTAM & Aircraft Cyber-Airworthiness Oversight | REFERENCE ONLY |
| FBI / IC3 | PIN 220420-2 — Ransomware Attacks on Agricultural Cooperatives (Private Industry Notification 220420-2) | FINAL |
| US FDA | 21 CFR 11 — Electronic Records; Electronic Signatures — 21 CFR Part 11 | FINAL |
| US FDA | 21 CFR 210/211 — Current Good Manufacturing Practice for Finished Pharmaceuticals — 21 CFR 210/211 | FINAL |
| US FDA | Medical Device Cybersecurity (FD&C Act §524B) | FINAL |
| US FDA | Drug Supply Chain Security Act (DSCSA) | FINAL |

| | | |
|---|---|---|
| US FDA | Food Safety Modernization Act (FSMA) — Preventive Controls (21 CFR 117), Intentional Adulteration/Food Defense (21 CFR 121) & Traceability Rule 204 | FINAL |
| FEMA | Homeland Security Exercise and Evaluation Program (HSEEP) | REFERENCE ONLY |
| Food and Ag-ISAC (with IT-ISAC) | Food and Agriculture Information Sharing and Analysis Center | REFERENCE ONLY |
| US FTA / APTA | FTA transit cybersecurity resources & APTA Recommended Practices | REFERENCE ONLY |
| Global Tailings Review (ICMM, UNEP, PRI) | Global Industry Standard on Tailings Management (GISTM) | REFERENCE ONLY |
| US HHS 405(d) | Health Industry Cybersecurity Practices (HICP) | FINAL |
| US HHS Office for Civil Rights | HIPAA Security Rule | FINAL |
| US HHS | Healthcare & Public Health Sector Cybersecurity Performance Goals (CPGs) | FINAL |
| International Association of Classification Societies (IACS) | IACS UR E26 & E27 — Cyber Resilience of Ships and Onboard Systems | REFERENCE ONLY |
| International Civil Aviation Organization | ICAO Annex 17 (Security) & Aviation Cybersecurity Strategy | REFERENCE ONLY |
| ICMM (International Council on Mining and Metals) | Critical Control Management (CCM) Good Practice Guide | REFERENCE ONLY |
| IEC / ISA | IEC 61511 (adopted in the US as ANSI/ISA-84) — Safety Instrumented Systems for the Process Industry | REFERENCE ONLY |
| International Maritime Organization (IMO) | IMO Resolution MSC.428(98) and Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) | REFERENCE ONLY |
| ISA / IEC | ISA-18.2 / IEC 62682 — Management of Alarm Systems for the Process Industries | REFERENCE ONLY |
| ISA/IEC | ISA/IEC 62443 Series — Security of Industrial Automation and Control Systems | REFERENCE ONLY |

| | | |
|---|---|---|
| ISO | ISO 17757:2019 — ISO 17757:2019 — Earth-moving machinery and mining: Autonomous & semi-autonomous machine system safety (ASAMS) | REFERENCE ONLY |
| ISO/IEC & CENELEC | ISO/IEC 22237 — ISO/IEC 22237 / EN 50600 — Data Centre Facilities & Infrastructure | REFERENCE ONLY |
| ISPE | GAMP 5 — A Risk-Based Approach to Compliant GxP Computerized Systems (2nd Edition) | REFERENCE ONLY |
| KNX Association | KNX Secure (KNX Data Secure & KNX IP Secure) | REFERENCE ONLY |
| Mining Association of Canada | Towards Sustainable Mining (TSM) | REFERENCE ONLY |
| MITRE | MITRE ATT&CK for ICS | FINAL |
| US Mine Safety and Health Administration (US DOL) | 30 CFR — MSHA Mine Safety Regulation — 30 CFR | FINAL |
| North American Electric Reliability Corporation (enforced by FERC) | NERC Critical Infrastructure Protection (CIP) Reliability Standards | REFERENCE ONLY |
| NERC Electricity Information Sharing and Analysis Center (E-ISAC) | E-ISAC and NERC GridEx | REFERENCE ONLY |
| NIST | NIST CSWP 29 2.0 — The NIST Cybersecurity Framework (CSF) 2.0 | FINAL |
| NIST | IR 8183 Rev. 2 — Cybersecurity Framework 2.0 Manufacturing Profile | INITIAL PUBLIC DRAFT |
| NIST | IR 8270 — Introduction to Cybersecurity for Commercial Satellite Operations | FINAL |
| NIST | IR 8374 Rev. 1 — Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile | FINAL |
| NIST | IR 8401 — Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control | FINAL |
| NIST | IR 8441 — Cybersecurity Framework Profile for Hybrid Satellite Networks | FINAL |
| NIST | NIST IR 8498 — Cybersecurity for Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems | FINAL |
| NIST NCCoE | SP 1800-10 — Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector | FINAL |

| | | |
|---|---|---|
| NIST NCCoE | SP 1800-41 — Responding to and Recovering from a Cyber Attack: Cybersecurity for the Manufacturing Sector | INITIAL PUBLIC DRAFT |
| NIST | SP 800-161 Rev. 1 — Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Rev. 1) | FINAL |
| NIST | SP 800-161 Rev. 1 (updated) — Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations | FINAL |
| NIST | SP 800-184 — Guide for Cybersecurity Event Recovery | FINAL |
| NIST | SP 800-61 Rev. 3 — Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile | FINAL |
| NIST | SP 800-82 Rev. 3 — Guide to Operational Technology (OT) Security | FINAL |
| US OSHA | Grain Handling Facilities — 29 CFR 1910.272 | FINAL |
| US OSHA | Process Safety Management of Highly Hazardous Chemicals (PSM) — 29 CFR 1910.119 | FINAL |
| US PHMSA | PHMSA Control Room Management Rule — 49 CFR 192.631 / 195.446 | FINAL |
| Space ISAC | Space Information Sharing and Analysis Center (resources and advisories) | REFERENCE ONLY |
| The White House | Space Policy Directive-5: Cybersecurity Principles for Space Systems | FINAL |
| US Transportation Security Administration (DHS) | TSA Cybersecurity Security Directives & Amendments (Airport and Aircraft Operators) | REFERENCE ONLY |
| US Transportation Security Administration | TSA Security Directives — Pipeline (SD Pipeline-2021-01 & -2021-02 series) | REFERENCE ONLY |
| US Transportation Security Administration | TSA Security Directives — Rail (SD 1580/82-2022-01 series) | REFERENCE ONLY |
| US Department of Defense (WBDG) | UFC 4-010-06 — Cybersecurity of Facility-Related Control Systems — UFC 4-010-06 | FINAL |
| US Chemical Safety and Hazard Investigation Board (CSB) | CSB Chemical Incident Investigations & Safety Recommendations | REFERENCE ONLY |
| US Coast Guard | Cybersecurity in the Marine Transportation System (final rule) & NVIC 01-20 | REFERENCE ONLY |
| USDA FSIS | | FINAL |

| | | |
|---|---|---|
| | Hazard Analysis and Critical Control Point (HACCP) Systems — 9 CFR Part 417 | |
| WaterISAC | Cybersecurity Fundamentals for Water and Wastewater Utilities | REFERENCE ONLY |

OT Crucible is an exercise, training, and resilience-planning platform. Exercise results do not constitute certification, legal advice, regulatory compliance determination, penetration testing, or a guarantee of cybersecurity.