Digital Training Resources (University of Navarra – IESE Business School)

From Humans to Machines: The Keys to Secure Digital Transformation

Project

TRANSFORM – Training and Re-skilling for Smart Manufacturing
Erasmus+ KA210-VET – Small-scale Partnerships in Vocational Education and Training
Project Reference: 2024-2-IE01-KA210-VET-000281740

Delivering Partner

University of Navarra – IESE Business School (Spain)

Activity Reference

Activity #2 – Collaborative Development

Resource Set Overview

This document presents **two complementary digital training resources developed by the University of Navarra (IESE Business School)**.

The resources are derived from IESE's contribution to the project and are designed for reuse in vocational education, executive education, and adult learning contexts.

RESOURCE 1

Digital Training Resource – From Humans to Machines: The Keys to Secure Digital Transformation

Resource Type

Modular Digital Training Resource (Reusable Learning Module)

Target Group

- Manufacturing managers and supervisors responsible for operational technology and production systems
- SME owners and decision-makers leading digital transformation initiatives
- Adult learners and professionals transitioning into leadership roles in smart manufacturing
- Executive education trainers and facilitators working with manufacturing organizations

EQF Level (indicative)

EQF Level 5–7 (Intermediate to advanced)

1. Purpose of the Resource

Funded by the European Union

This digital training resource addresses the critical intersection of digital transformation, cybersecurity, and privacy in smart manufacturing. As manufacturing organizations adopt Industry 4.0 technologies—including IoT, AI, cloud-based automation, robotics, and connected systems—they face unprecedented cybersecurity risks and privacy challenges that threaten operational continuity and digital trust.

The resource equips learners with both technical competencies (understanding OT/IT vulnerabilities, risk assessment frameworks) and managerial competencies (governance, strategic decision-making, organizational change management) necessary to secure digital transformation initiatives.

Based on real-world manufacturing cyberattacks and emerging threat landscapes, this resource emphasizes:

- Digital transformation in manufacturing and its strategic implications
- The convergence of Operational Technology (OT) and Information Technology (IT) systems
- Practical risk management strategies for Industry 4.0 environments
- The critical role of human factors in cybersecurity resilience
- Hands-on simulation experience to understand attack vectors and defense mechanisms

2. Learning Objectives

After completing this resource, learners will be able to:

1. Understand the fundamentals of digital transformation in manufacturing and identify strategic opportunities and challenges when integrating Industry 4.0 technologies
2. Explain the convergence of IT and OT systems and assess the cybersecurity implications for smart manufacturing environments
3. Apply risk management frameworks (NIST CSF, IEC 62443, ISO 27001) to identify, assess, and prioritize cybersecurity risks in Industry 4.0 contexts
4. Recognize human factors as critical vulnerabilities in cybersecurity and develop strategies to enhance organizational resilience through training and awareness
5. Navigate data privacy regulations and ethical considerations when deploying connected systems and analytics in manufacturing
6. Develop practical incident response capabilities through scenario-based simulations and tabletop exercises
7. Lead organizational change initiatives that integrate cybersecurity considerations into digital transformation strategy and culture

3. Structure and Content

Module 1: Leading Digital Transformation in Manufacturing

Duration: 1 hour 15 minutes

Module Overview

This foundational module introduces participants to digital transformation in manufacturing through the Italgas case study. It explores how organizations build technological, organizational, and people capabilities while developing a digital factory mindset. The module establishes the critical connection between digital transformation strategy and cybersecurity imperatives, setting the stage for deeper exploration in subsequent modules.

Key Topics

1. Building Technological Capabilities for Industry 4.0

- Overview of Industry 4.0 technologies: IoT, cloud computing, AI/ML, digital twin, robotics
- Technology infrastructure requirements and integration challenges
- Italgas case: Technology stack and digital infrastructure deployment

2. Organizational and People Capabilities

- Organizational restructuring for digital transformation
- Workforce upskilling and digital literacy initiatives
- Italgas case: Talent development and organizational change management

3. Digital Factory Mindset and Cybersecurity Foundations

- Cultivating a culture of innovation and continuous improvement
- Introduction to cybersecurity as a strategic enabler of digital transformation
- Italgas case: Integrating security-by-design principles in digital initiatives

Funded by the European Union

IESE Business School University of Navarra

Module 2: OT/IT Convergence in Smart Manufacturing

Duration: 1 hour 15 minutes

Module Overview

This module examines the convergence of Operational Technology (OT) and Information Technology (IT) systems in manufacturing environments. Participants explore the technical, governance, and security challenges that arise from integrating traditionally isolated OT systems with connected IT infrastructure. Real-world incidents demonstrate the expanding attack surface and the strategic importance of unified cybersecurity governance.

Key Topics

1. Understanding OT/IT Systems and Their Convergence

- Fundamentals of OT: SCADA, ICS, PLCs, and industrial control systems
- IT systems in manufacturing: ERP, MES, data analytics platforms
- Drivers and benefits of OT/IT convergence in Industry 4.0

2. Cybersecurity Challenges in Converged Environments

- Expanded attack surface: vulnerabilities introduced by connectivity
- Legacy OT systems and lack of security controls
- Case study: Jaguar Land Rover ransomware attack and production disruption

3. Integrated Security Governance Across OT/IT

- Developing unified security policies and procedures
- Network segmentation and zero-trust architecture principles
- Introduction to IEC 62443 standard for industrial automation and control systems

Funded by the European Union

IESE Business School University of Navarra

Module 3: Risk Management in Cybersecurity for Industry 4.0

Duration: 1 hour 15 minutes

Module Overview

This module equips participants with practical cybersecurity risk management strategies tailored to smart manufacturing environments. Learners explore industry-standard frameworks, conduct risk assessments, and prioritize cybersecurity investments aligned with business objectives. The module emphasizes balancing innovation with security in the context of cloud, IoT, AI, and robotics adoption.

Key Topics

1. Cybersecurity Risk Assessment Frameworks

- Overview of NIST Cybersecurity Framework (CSF): Identify, Protect, Detect, Respond, Recover
- ISO 27001 information security management principles
- Risk-based prioritization: likelihood, impact, and business criticality

2. Managing Risks in Industry 4.0 Technologies

- Cloud security: shared responsibility model and data sovereignty
- IoT and connected devices: authentication, encryption, firmware security
- AI/ML security: adversarial attacks, data poisoning, model integrity
- Third-party and supply chain risks in digital ecosystems

3. Strategic Cybersecurity Investment and Governance

- Aligning cybersecurity with business strategy and digital transformation goals
- Building a cybersecurity governance structure: roles, responsibilities, and accountability
- Metrics and KPIs for measuring cybersecurity effectiveness

Funded by the European Union

IESE Business School University of Navarra

Module 4: The Human Factor and Data Privacy Protection

Duration: 1 hour 15 minutes

Module Overview

This module addresses the critical role of human behavior in cybersecurity resilience and the complex challenges of data privacy in connected manufacturing environments. Participants examine why humans remain the weakest link in security and how to strengthen organizational defenses through awareness, training, and culture change. The module also explores privacy regulations and ethical considerations as humans and machines become increasingly interconnected.

Key Topics

1. Human Vulnerabilities in Cybersecurity

- Social engineering, phishing, and insider threats
- Case studies: Aviation and airport cyber disruptions driven by human error
- Behavioral economics and decision-making under uncertainty

2. Building a Security-Aware Culture

- Designing effective cybersecurity awareness and training programs
- Simulated phishing exercises and incident response drills
- Leadership's role in championing cybersecurity culture

3. Data Privacy and Ethical Considerations

- GDPR and privacy regulations in manufacturing contexts
- Data minimization, consent, and transparency in IoT deployments
- Balancing data utilization for optimization with privacy protection

Funded by the European Union

IESE Business School University of Navarra

Module 5: Change Management and Leadership in Secure Digital Transformation

Duration: 1 hour 15 minutes

Module Overview

This capstone module synthesizes learning from previous modules and focuses on leading organizational change that integrates cybersecurity into digital transformation strategy. Participants develop skills to navigate resistance, align stakeholders, and embed security thinking into organizational culture and decision-making processes. The module emphasizes the leadership competencies required to drive sustainable, secure digital transformation.

Key Topics

1. Change Management Principles for Digital Transformation

- Understanding organizational change: models and frameworks (Kotter, ADKAR)
- Identifying and managing resistance to digital and security initiatives
- Communication strategies for building buy-in across the organization

2. Leadership Competencies for Secure Digital Transformation

- Strategic vision: aligning technology, people, and processes
- Cross-functional collaboration: bridging IT, OT, security, and business units
- Decision-making in complex, uncertain environments

3. Embedding Cybersecurity into Organizational Culture

- Creating accountability structures and security champions programs
- Continuous improvement: measuring progress and adapting to evolving threats
- Developing a roadmap for sustainable secure digital transformation

4. Learning Activities

This digital training resource incorporates diverse, hands-on learning experiences across all five modules:

- **Case Study Analysis:** Real-world cases in manufacturing and cybersecurity: Italgas, Jaguar Land Rover ransomware, aviation cyber disruptions.
- **Interactive Simulations & Tabletop Exercises:** Harvard-style cyber attack simulation, OT/IT vulnerability identification, risk assessment scenarios.
- **Group Discussions & Workshops:** Collaborative activities on investment prioritization, change management planning, and stakeholder alignment.
- **Reflection & Self-Assessment:** Organizational digital maturity and leadership readiness evaluation exercises.

5. Format and Accessibility

This resource may be delivered and reused in multiple digital formats, including:

- Slide deck with facilitator notes
- PDF learning pack

Funded by the European Union

IESE Business School University of Navarra

RESOURCE 2

Recorded Webinar Learning Module

Resource Type

Recorded webinar-based digital training module

Delivery Context

Derived from the **IESE-led project webinar** titled **"From Humans to Machines: The Keys to Secure Digital Transformation"**, focusing on securing digital transformation in manufacturing.

1. Purpose of the Resource

The purpose of this resource is to enable learners to engage on the important topic of IT/OT cybersecurity, risk management, and human factors in smart manufacturing environments.

2. Learning Objectives

After completing this learning module, learners will be able to:

1. Explain the challenges of OT/IT convergence and its impact on cybersecurity in manufacturing
2. Identify practical risk management strategies for Industry 4.0 technologies (cloud, IoT, AI, robotics)
3. Recognize human vulnerabilities in cybersecurity and data privacy protection requirements
4. Assess cybersecurity implications for their own organizational digital transformation initiatives

3. Core Learning Content

- Webinar recording (60 minutes, on-demand video)
- Presentation slides highlighting the webinar structure and themes

4. Structured Learning Guide

Key Topics Covered

- OT/IT convergence in smart manufacturing
- Cybersecurity risk management for Industry 4.0
- Human factors and data privacy protection

5. Learning Activities

- **Individual reflection:** Assess OT/IT cybersecurity gaps in your organization
- **Group discussion (optional):** Analyze webinar case studies (Jaguar Land Rover, aviation disruptions)
- **Practical task (optional):** Identify leadership actions to strengthen cybersecurity governance.

7. Licensing and Reuse

This document constitutes digital training resources developed by the University of Navarra – IESE Business School under the Erasmus+ KA210-VET project TRANSFORM and may be used as evidence of project outputs in interim and final reporting.