Cybersecurity I

Student Guide

Dr Diarmuid Ó Briain

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Table of Appreviations

2FA	Two-Factor Authentication
AAA	Authentication, Authorisation, Accounting
ACK	ACKnowledge
ACL	Access Control List
ACS	Annual Cost of Safeguard
AI	Artificial Intelligence
AIC	Availability, Integrity, Confidentiality
ALE	Annualised Loss Expectancy
APO	Align, Plan and Organise
ARO	Annualised Rate of Occurrence
ARP	Address Resolution Protocol
AS	Authentication Server
AV	Asset Value
BAI	Build, Acquire and Implement
BCP	Business Continuity Plan
BMS	Building Management Systems
CA	Companies Act
CBA	Cost Benefit Analysis
CBI	Central Bureau of Investigation
CC	Common Criteria
CCPA	California Consumer Privacy Act
CCRA	Common Criteria Recognition Arrangement
CCTV	Close Circuit TeleVision
CDN	Content Deliver Network
CEO	Chief Executive Officer
CER	Crossover Error Rate
CERT-In	Indian Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act
CIA	Confidentiality, Integrity, Availability
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMA	Computer Misuse Act
CMM	Capability Maturity Model
CNI	Critical National Infrastructure
COBIT	Control Objectives for Information and Related Technology
COBOL	COmmon Business-Oriented Language
COCOM	Coordinating Committee for Multilateral Export Controls
CoE	Council of Europe
COO	Chief Operating Officer
COPPA	Children's Online Privacy Protection Act
COSO	Committee of Sponsoring Organisations
CP	Controls points

CSF	Cybersecurity Framework 2.0
CSO	Chief Security Officer
DAC	Discretionary Access Controls
DCS	Distributed Control Systems
DE	Detect
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DiD	Defence-in-Depth
DMZ	De-Militarised Zone
DNP3	Distributed Network Protocol version 3
DORA	Digital Operational Resilience Act
DoS	Denial of Service
DPA	Data Protection Authority
DPDP	Indian Digital Personal Data Protection Act
DSP	Digital Service Providers
DSS	Data Security Standard
DSS	Deliver, Service and Support
DVR	Digital Video Recorders
EAR	Export Administration Regulations
ECO	Export Control Order
EDM	Evaluate, Direct and Monitor
EF	Exposure Factor
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
ESB	Electricity Supply Board
FAR	False Acceptance Rate
FBI	Federal Bureau of Investigation
FCPA	US Foreign Corrupt Practices Act
FCRA	air Credit Reporting Act
FCS	Fire Control Systems
FISMA	Federal Information Security Modernization Act
FRR	False Rejection Rate
GCHQ	UK's Government Communications Headquarters
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GSLB	Global Server Load Balancing
GV	Govern
HIDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HMI	Human Machine Interfaces
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilating, and Air Conditioning
IACS	Industrial, Automation and Control Systems
ICIF	Internal Control - Integrated Framework
ICMP	Internet Control Message Protocol

ICS	Industrial Control System
ICT	Information Communications Technology
ID	IDentification
ID	Identify
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
IOT	Internet of Things
IP	Internet Protocol
IPC	Indian Penal Code 1860
IPC	Industrial PC
IPS	Intrusion Prevention System
IRP	Incident Response Plan
IRT	Isochronous Real-Time
IS	Information Systems
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
IT	Information Technology
ITADA	Identity Theft and Assumption Deterrence Act
ITAM	IT Asset Management
ITIL	IT Infrastructure Library
ITSM	IT Service Management
KDC	Key Distribution Centre
LBAC	Lattice-based Access Control
MAC	Mandatory Access Control
MEA	Monitor, Evaluate and Assess
MeitY	Ministry of Electronics and Information Technology
MERCOSUR	MERcado COmún del SUR Southern Common Market
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
MLS	Multi-Level Secure
MO	Modus Operandi
MOM	Opportunity and Motives
NAFTA	North American Free Trade Agreement
NAT	Network Address Translation
NCSC	National Cyber Security Centre
NDA	Non-Disclosure Agreements
NIDS	Network-based IDS
NIDS	Network Intrusion Detection Systems
NIS2	Network Information Systems version 2
NIST	National Institute of Standards and Technology
NMAP	Network Mapper

nonce	Number used ONCE
NPSA	National Protective Security Authority
NSE	NMAP Scripting Engine
NT	Network Technician
NTP	Network Time Protocol
NVR	Network Video Recorders
OES	Operators of Essential Services
OGC	Office of Government Commerce
OS	Operating Systems
OT	Operational Technology
OTP	One Time Password
OTSec	OT Security
PACS	Physical Access Control Systems
PC	Personal Computer
PCI	Payment Card Industry
PECR	Privacy and Electronic Communications
PID	Proportional-Integral-Derivative
PIDS	Protocol-based Intrusion Detection System
PIN	Personal Identification Number
PING	Packet InterNet Groper
PLC	Programmable Logic Controller
POCA	Prevention of Corruption Act
PPE	Personal Protective Equipment
PR	Protect
Profinet	Process Field Network
RADIUS	Remote Access Dial-in User Service
RBAC	Role-based Access Control
RC	Recover
RDM	Remote Diagnostics & Maintenance
RMP	Risk Management Plan
RS	Respond
RTOS	Real Time Operating System
RTU	Remote Terminal Units
SAML	Security Assertion Markup Language
SBU	Sensitive but Unclassified
SCADA	Supervisory Control and Data Acquisition
SCTP	Stream Transmission Control Protocol
SCTP	Stream Control Transmission Protocol
SEC	Securities and Exchange Commission
SFO	Serious Fraud Office
SIS	Safety Instrumented Systems
SLA	Service Level Agreements
SLE	Single Loss Expectancy
SME	Subject Matter Expert
SMS	Short Messaging Service

SMT	Senior Management Team
SoD	Separation of Duties
SoP	Separation of Powers
SP	Special Publication
SRT	Soft-Real Time
SS	Service Server
SSH	Secure Shell
SSO	Single Sign On
SYN	SYNchronise
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TGS	Ticket Granting Server
TOR	The Onion Router
TSN	Time-Sensitive Networking
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VCDPA	Virginia Consumer Data Protection Act
WTO	World Trade Organisation

Module Aim

Provide learners with the ability to combine Operational Technology (OT) Industrial Automation and Control Systems (IACS) and protocols with Cybersecurity frameworks and tools in order to prepare the model for incident response plans to counteract the cyber attacks.

Learning Outcomes

On successful completion of this module the learner should be able to:

- Visualise Industrial Automation and Control System (IACS) as they are employed in manufacturing, distribution and critical infrastructure.
- Construct a business case for Security of an IACS.
- Consider Cyber Security Architectures applicable to the security of IACS.
- Categorise physical and digital access controls as they apply to the security of an IACS.
- Appraise risk management, risk assessment and the execution of risk management tasks in the context of IACS security.

Supplementary Book Resources

Pascal Ackerman 2017, Industrial Cybersecurity, Packt Publishing Ltd [ISBN: 9781788395984]

Eric D. Knapp,Joel Langill 2014, Industrial Network Security, Syngress Press [ISBN: 0124201148]

Edward J. M. Colbert,Alexander Kott 2018, Cyber-security of SCADA and Other Industrial Control Systems, 1 Ed., 16, Springer

[ISBN: 3319812033]

Recommended Article/Paper Resources

US National Institute of Standards and Technology (NIST) 2022, Guide to Industrial Control Systems Security Revision 2, Special Publication, NIST SP 800-82.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

US National Institute of Standards and Technology (NIST) 2015, Guide to Operational Technology (OT) Security Revision 3, Initial Public Draft, NIST SP 800-82r3 ipd.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf

US National Institute of Standards and Technology (NIST) 2020, Security and Privacy Controls for Information Systems and Organizations to OT', NIST SP 800-53 Rev. 5.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf

Abstract

This module explores cybersecurity on Operational Technology (OT), it will cover some of the basic OT and fundamentals of OT security by putting OT into real-world context, both from an industry standpoint and everyday life. The course will begin by considering some of the recent history of OT, how they've evolved into the types of complex industrial environments that exist today, and some examples of how some of the devices that make up control systems actually work. This will be followed by a a deeper dive into those devices as well through examples, real-world context. This will be followed lead to some of the industry-standard frameworks and standards that are commonly used when we're applying controls to OT networks such as those from the US National Institute of Standards and Technology (NIST), the Purdue Network Reference Model, International Society of Automation (ISA) 62443 and the MITRE ATT&CK. The module will progress to consider convergence and its importance within the OT space, convergence meaning IT, OT, and security coming together to protect, control and secure those systems. Finally the module will work through the steps to respond to a breach, what to do when a breach occurs on the OT network.