

Theme 1 Pre-Reading Packet: Foundations, History & Taxonomy



Dr Diarmuid Ó Briain
Version: 1.0

Copyright © 2026 C²S Consulting

Licensed under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



Table of Contents

1 Objectives.....	4
2 Introduction.....	4
3 Cybersecurity terms and Concepts.....	5
3.1 Asset.....	5
3.2 Threat.....	5
3.3 Vulnerability.....	6
4 Risk.....	6
4.1 Risk Management.....	6
5 Critical Infrastructure Sectors.....	7
5.1 Critical Infrastructure.....	7
6 Critical Evolutions in OT.....	9
6.1 Industrial Revolution.....	9
6.2 Early Age of Computing.....	9
6.3 Computing after World War 1.....	10
6.4 Computing and Industrial Control.....	10
7 Evolution of Operational Technology.....	11
8 Access Control.....	12
8.1 Preventive access control.....	12
8.2 Deterrent access control.....	12
8.3 Detective access control.....	12
8.4 Corrective access control.....	12
8.5 Recovery access control.....	12
8.6 Compensation access control.....	12
8.7 Directive access control.....	13
8.8 Administrative access control.....	13
8.9 Logical or technical access control.....	13
8.10 Physical access control.....	13
9 Bibliography.....	14

Illustration Index

Figure 1: Risk example.....	5
Figure 2: ESB Aghada gas fired Power Station, Cork, Ireland.....	8
Figure 3: From loom to computer.....	9
Figure 4: 1950s: Computer paper tape used to store programs.....	10
Figure 5: Siemens PLCs from 1958 to today.....	10
Figure 6: ESB "Smart" meter.....	11

1 Objectives

By the end of this Pre-Reading Packet (PRP), you will be able to:

- Define and differentiate the core components of the cybersecurity triad: Assets, Threats, and Vulnerabilities.
- Understand the basic concept of risk and how organizations approach fundamental risk management.
- Identify the critical infrastructure sectors that rely heavily on industrial automation.
- Trace the historical evolution of information processing from the Industrial Revolution to modern industrial control systems.
- Classify physical and digital security measures into their appropriate functional access control categories.

 **Important Notice for Students:** This document contains the foundational definitions and history required for Theme 1. You are expected to master this material independently. This material will be directly tested in the Session 4 Individual Readiness Assurance Test (iRAT).

2 Introduction

In modern enterprise architecture, cybersecurity is no longer confined to safeguarding databases, corporate email servers, and web applications. It extends deep into physical operations, controlling water treatment plants, electrical grids, manufacturing assembly lines, and rail systems.

To effectively protect these highly specialised environments, a shared technical vocabulary must be established as well as an understand the history that brought us here. This PRP is designed to give that foundation before stepping into live interactive lectures.

Rather than spending valuable class time reciting basic definitions, we expect you to master this core taxonomy independently. By doing so, the live sessions can focus on complex engineering architectures, protocol breakdowns, and hands-on defence strategies.

3 Cybersecurity terms and Concepts



Figure 1: Risk example

3.1 Asset

In almost any context, an asset is a positive thing, and it often has worth. Money is an asset, for example. When you list assets and liabilities, assets are all things that have value. In broad terms, an asset can be people, property, or information. But it can also include your online reputation or a database of customer information. A machine within an industrial setting is also an asset. Anything that has a value to the owner and needs to be protected is an asset.

3.2 Threat

Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the nation through an information system via unauthorised access, destruction, disclosure, modification of information, and/or Denial of Service (DoS).

3.3 Vulnerability

The only way a threat can do damage to an asset is if the asset has an unchecked vulnerability that the threat can take advantage of. In the house example, a vulnerability could be a security system that relies on electricity. If there is no battery backup, the burglar could take down the power and then have free access to the home. Another vulnerability could be something as simple as an unlocked window. Anything that a burglar could take advantage of is a vulnerability.

By that same token, in an industrial setting a Programmable Logic Controller (PLC) can have vulnerabilities that hackers can take advantage of. Legacy PLC's that are not updated or maintained can be as dangerous as they can an access to a facility, equipment or service. If firmware is not updated regularly, then vulnerabilities can be made available for hackers to gain access. Put all of this together, and there is risk.

4 Risk

Risk is the potential for loss, damage or destruction of an **asset** as a result of a **threat** exploiting a **vulnerability**. Risk is a function of threats taking advantage of vulnerabilities to steal or damage assets. Understanding these separate concepts helps to understand how safe an industrial environment really is. Threats, like hackers, may exist. But if there are no vulnerabilities within the people, processes or technology of the environment, then risk is very low. Vulnerabilities may exist in the environment, but if threats do not exist, then there is still little risk (this is not really an option, however, as hackers are very prevalent online). For industrial cybersecurity, the goal is to close off any vulnerabilities so that assets remain safe.

4.1 Risk Management

From the point of view of risk management there are a number of ways in which risks can be treated, these include:

Risk Acceptance

- Management deem the risk acceptable, compared to the cost of implementing controls to mitigate against it.

Risk Mitigation

- Implement a suitable control or combination of controls to reduce (mitigate) the risk to an acceptable level.

Risk Avoidance

- Avoiding the risk all together making a decision not to enter into the associated activity.

Risk Transfer

- Transfer the risk to another organisation. For example, purchasing of insurance for equipment.

5 Critical Infrastructure Sectors

Most countries define and specify their critical infrastructures and often group them into sectors. In terms of actual industrial control systems, one major factor that determines how systems are architected and secured is regulation.

5.1 Critical Infrastructure

The EU, the UK and the US group and define critical infrastructure sectors differently; however, all three contain the same facilities, just defined differently.

5.1.1 In the EU

The EU Network Information Systems version 2 (NIS2) [1] and Resilience of Critical Entities [2] directives group sectors of high criticality as:

- Energy
 - *Electricity*
 - *District heating and cooling*
 - *Oil*
 - *Gas*
 - *Hydrogen*
- Transport
 - *Air*
 - *Rail*
 - *Water*
 - *Road*
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (business-to-business)
- Public administration
- Space

Figure 2 is an example of a Critical Entity, it is an Electricity Supply Board (ESB) gas-powered electrical generation station that supplies electricity to Cork City, Ireland.

Further to these high critical sectors there are other critical sectors defined as follows:

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing
- Digital providers
- Research



Figure 2: ESB Aghada gas fired Power Station, Cork, Ireland

5.1.2 In the UK

The UK Cabinet Office has, through the National Protective Security Authority (NPSA), defined 13 National Infrastructure sectors [3]. Several sectors have defined sub-sectors; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard. The sectors are:

- Chemicals
- Civil Nuclear Communications
- Defence
- Emergency Services
- Energy
- Finance
- Food
- Government
- Health
- Space
- Transport
- Water

6 Critical Evolutions in OT

6.1 Industrial Revolution

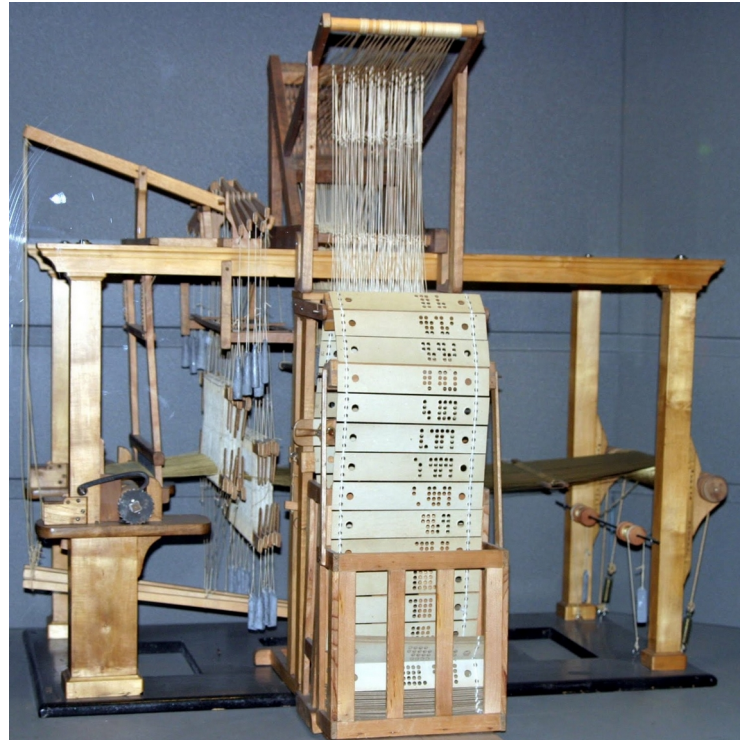


Figure 3: From loom to computer

The increase in complexity of industrial automation over the past century has seen greater efficiencies and the production of utilities and products at lower costs. Looking back there are many examples of the introduction of automation, for example the introduction of punchcards readers in textile looms, in the North of England in the mid 1800s, led to the automation of pattern weaving thereby reducing labour costs and increasing output.

6.2 Early Age of Computing

Ada Lovelace took the idea and applied it to write programs for Charles Babbage's Analytical engine [4]. More recent examples include the use of gyroscopes that were designed for aircraft autopilots during the first decade of the 20th century. The biggest advances in early control system technology occurred during the pre-World War II period and actually during the war itself. This was to solve problems associated with things like tracking targets and platform stability. Consider aircraft bomb aimers looking at a bomb sight, these were stabilised control systems.

6.3 Computing after World War 1

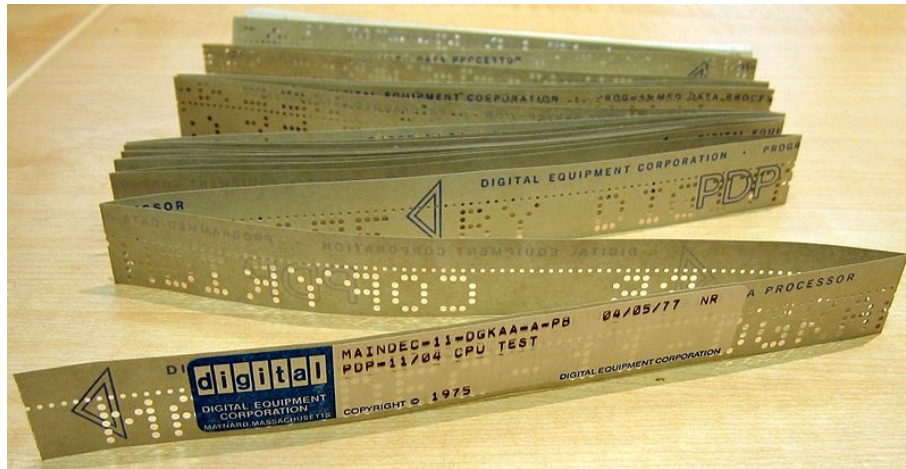


Figure 4: 1950s: Computer paper tape used to store programs

The computer control systems that we know today are very closely linked to the invention of the first data processing machines, the precursor to modern computers. The punch tape that Ada Lovelace made use of in the mid-1800s was still in use with mainframes in the 1950s with COMmon Business-Oriented Language (COBOL) software.

6.4 Computing and Industrial Control

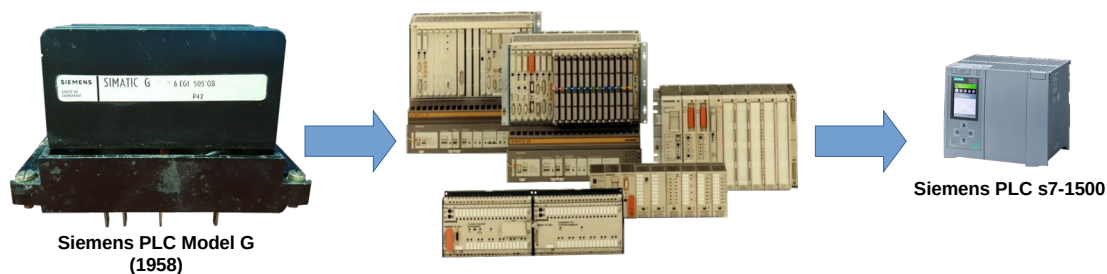


Figure 5: Siemens PLCs from 1958 to today

PLC, first came into play in the 1960s within the car manufacturing industry to manage the frequent changes in the configuration of the machines that were used on the production lines. The main problem with them was that factory floor workers needed to learn computer programming, sometimes in low-level languages such as assembler, to operate and troubleshoot them. However, when it was first realised that many of the factory electricians were familiar with ladder logic, changes were made to the way that PLCs were developed to make them easier to program, and ladder logic became the principal means of programming a PLC, as it is today. The first modern PLCs were made during the late 1960s, and they began to be widely deployed by electrical and gas utility and pipeline companies, and in turn leading to the development of SCADA systems for controlling and monitoring PLCs over a large geographic area.

7 Evolution of Operational Technology

OT has continued to evolve as IT capabilities are inserted into existing physical systems. In many cases these replace or supplement physical control mechanisms. This evolution has been encouraged through the improvements in both cost and performance and this has led to the “smart” technologies we have today.



Figure 6: ESB "Smart" meter

For example the electricity meters in homes across Ireland have been replaced with “smart” meters. These “smart” meters benefit the ESB as they give accurate real-time readings and are more difficult to tamper with. The consumer benefits too as “smart” meters measures electricity usage without the need for estimated meter readings and they will only reflect the electricity actually used. The consumer no longer have to submit readings or have someone read the meter. These meters also provide the consumer with greater access to accurate information on energy usage, and therefore the consumer has greater control over their energy consumption. By changing behaviour based on more insightful insights, the consumer can reduce bills as well as their carbon footprint.

Engineering models and analysis are evolving to address these emergent properties, including safety, security, privacy, and environmental impact interdependencies.

8 Access Control

Access Controls protect Confidentiality, Integrity and Availability (CIA) of objects¹.

8.1 Preventive access control

Stop unwanted or unauthorised activity from occurring. These include biometrics, fences and locks, data classification, job rotation and Separation of Duties (SoD) plus auditing, cryptography and monitoring.

8.2 Deterrent access control

Discourages the violation of security policies, often filling the gap left by preventive controls. They include gates, keyed access and security guards, badges, cameras and intrusion alarms or awareness training, separation of duties and security clearances.

8.3 Detective access control

Discovers unwanted or unauthorised activity but often take effect after an incident has occurred as opposed to before or during its occurrence. Security patrols, Security badges, guard dogs, security cameras, motion detectors and sound alarms or incident investigations, supervisory review, audits, and violation or exception reports.

8.4 Corrective access control

These restore systems to a known-good state following a security-related breach or incident. Access termination, service restarting or system rebooting, the implementation of Intrusion Detection Systems (IDS), antivirus programs and malware scanners, Business Continuity Plan (BCP), Disaster Recovery (DR) planning and security policies are typical corrective access controls.

8.5 Recovery access control

These are used to repair and restore critically damaged capabilities, functions and resources following a security violation. These are more complex in scale and scope than corrective controls and include backups, rollbacks and restorations, fault-tolerance, redundancy and clustering, or antivirus scanners, database shadowing and data replication.

8.6 Compensation access control

This provides aid to various other existing controls in the enforcement of system-wide security policies. This includes security policies, operational requirements or utilisation criteria or personnel supervision, monitoring and work procedures.

1 Object – Computer/system that may be accessed.

8.7 Directive access control

This confines and controls the actions of subjects² to enforce and encourage strict security policy compliance. Security guards, guard dogs and security cameras, policy requirements, security criteria and posted notifications, or escape routes, employee supervision and awareness training all come under the umbrella of directive access control.

8.8 Administrative access control

This is the defined policies and procedures of the organisation that governs overall access, focusing on personnel and business practices. Workplace policies, procedures and hiring practices, background checks, data classification and security training or work reviews, employee supervision and personnel controls are examples.

8.9 Logical or technical access control

These are hardware and software mechanisms that manage access to and provide protection for shared computer and network resources. Encryption, passwords and smartcards, access control lists, biometrics and constrained interfaces or cryptographic protocols, firewall appliances and network routers.

8.10 Physical access control

These are structural barriers emplaced to prevent direct access to components of a facility, network or system. Security guards, guard dogs and fences, alarm systems, motion detectors and security windows or security lights, security locks and video cameras.

² Subject – S/he who may try and access the object.

9 Bibliography

- [1] Directive (EU) 2022/2555, *EU Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [2] Directive (EU) 2022/2557, *EU The resilience of critical entities and repealing Council Directive 2008/114/EC*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: <http://data.europa.eu/eli/dir/2022/2557/oj>
- [3] 'Public Summary of Sector Security and Resilience Plans'. UK Cabinet Office, Feb. 01, 2019. Accessed: Aug. 08, 2023. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf
- [4] L. F. Menabrea and A. Lovelace, 'Sketch of The Analytical Engine', *Bibliothèque Universelle de Genève*, Oct. 1842, Accessed: Aug. 08, 2023. [Online]. Available: <https://www.fourmilab.ch/babbage/sketch.html>