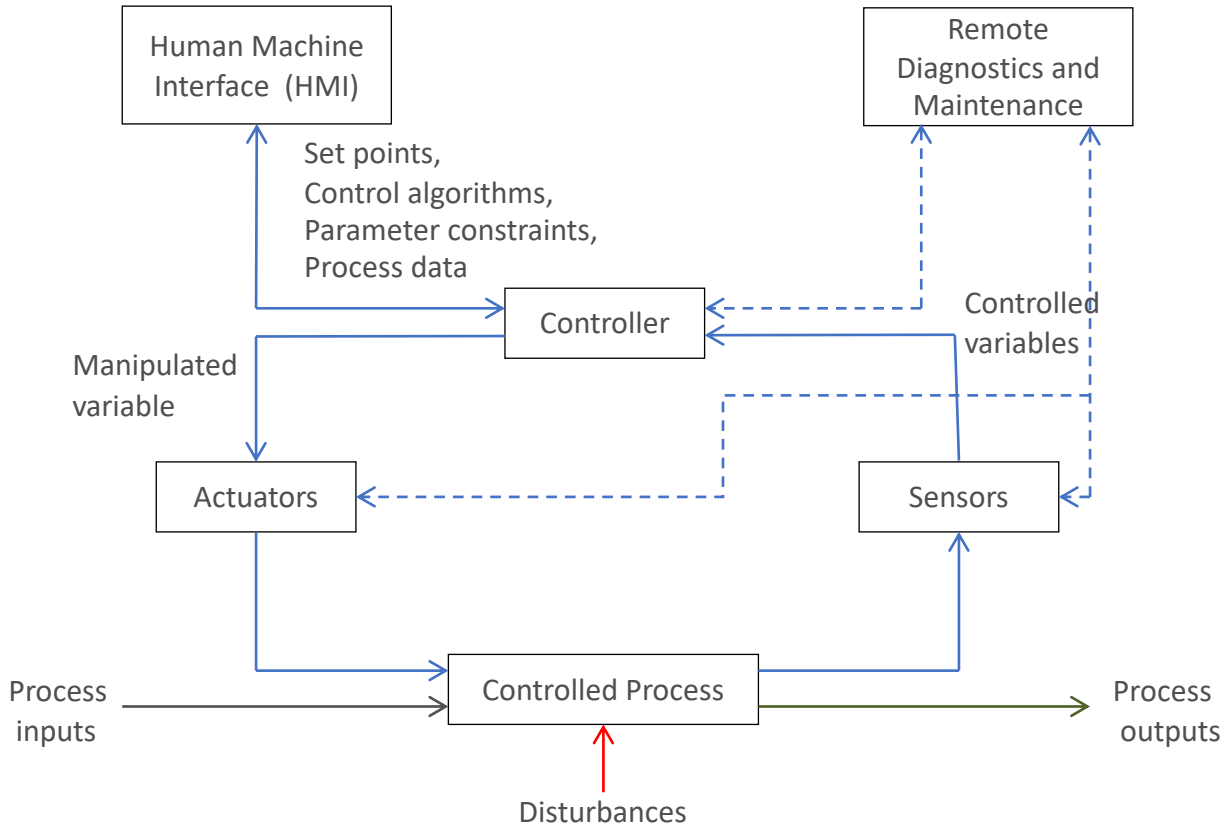
Industrial Control Systems

Chris Hankin

Generic ICS Architecture



Glossary

- DCS: Distributed Control System – intelligence gathering throughout controlled process
- IED: Intelligent Electronic Device
- PLC: Programmable Logic Controller
- RTU: Remote Terminal Unit – a computer with radio interfacing
- SIS: Safety Instrumented System
- SCADA: Supervisory Control and Data Acquisition

CNI Sectors (UK)

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

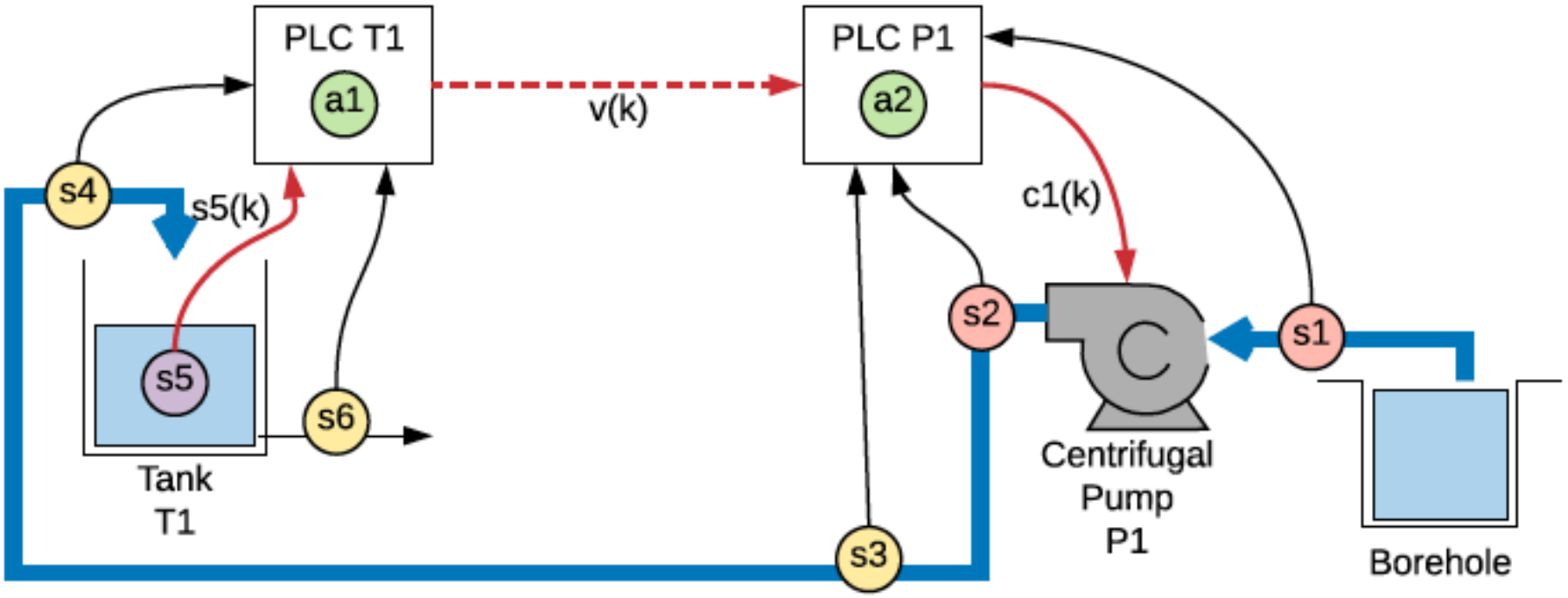
Control Components

- SCADA, DCS and PLCs
- Electrical – for example, sensors
- Mechanical – for example, valves
- Hydraulic – for example, hydraulic presses
- Pneumatic – for example in HVAC control systems

ICS Industrial Sectors

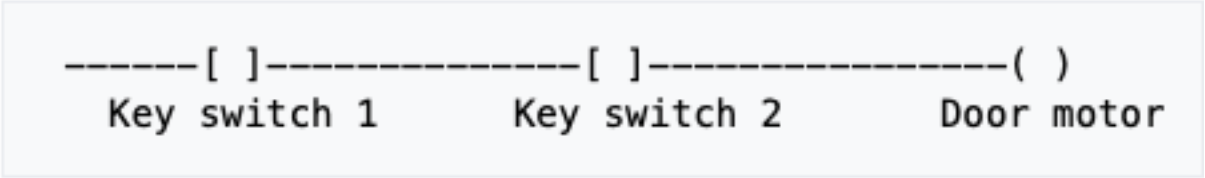
- Manufacturing
  - Process-based:
    - Continuous Processes – for example, petroleum in a refinery or distillation in a chemical plant.
    - Batch Manufacturing – distinct start and end point, for example in food production.
  - Discrete: parts assembly and machining
- Distribution industries – typical in critical infrastructure (for example power or water distribution).
- Difference in geographic spread: manufacturing normally localized.

Water Distribution

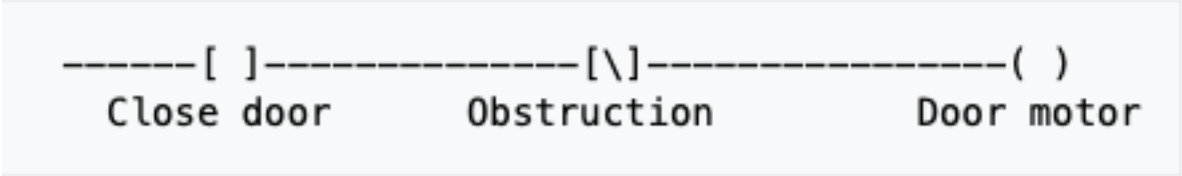


Ladder Logic (Wikipedia)

AND



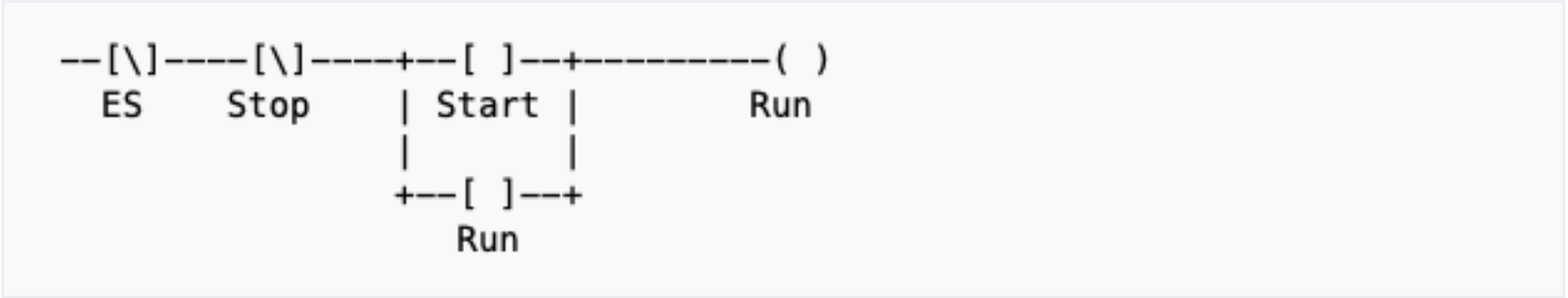
NOT

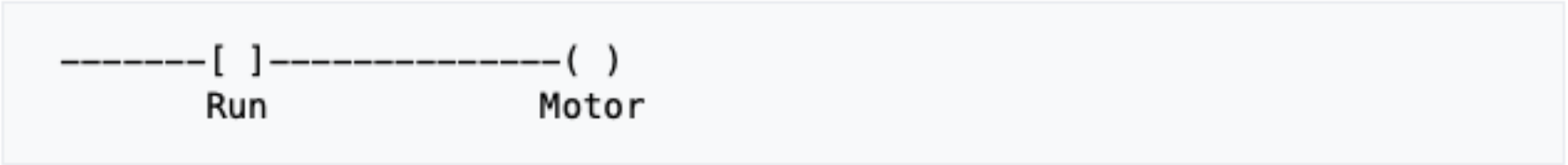


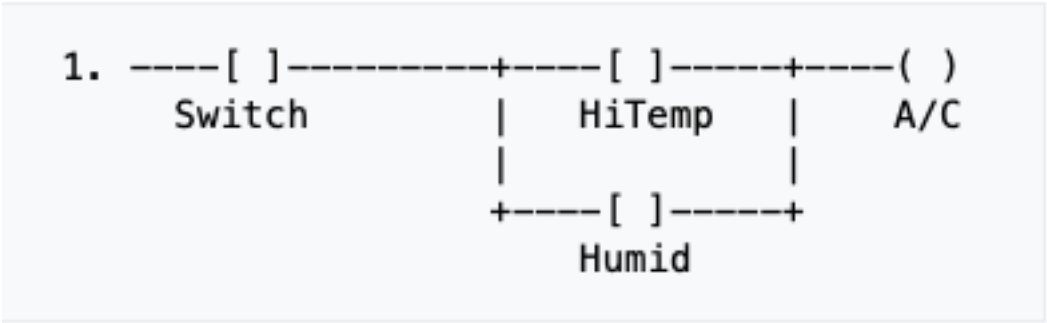
OR

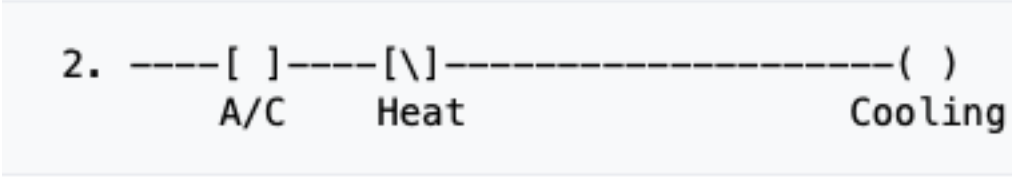
[ ] input ( ) output

Continued



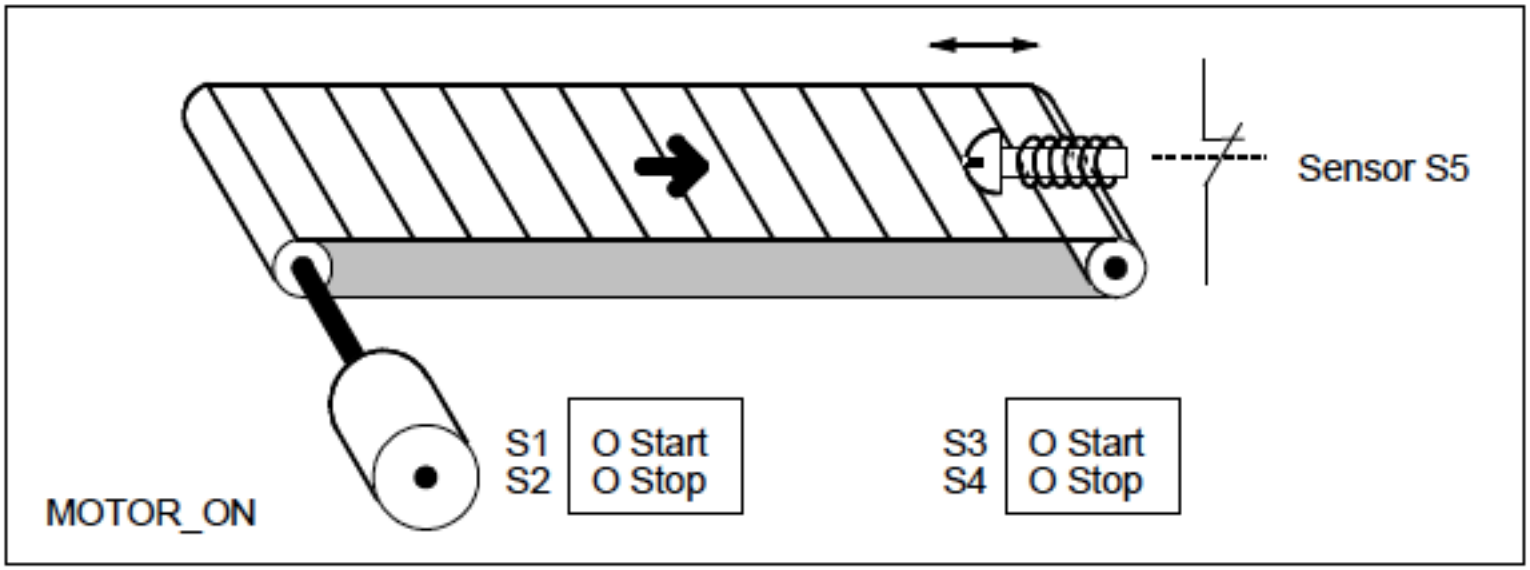


1. 

2. 

Siemens Step 7

Mnemonic	Program Elements Catalog	Description
AW	Word logic instruction	And Word
OW	Word logic instruction	Or Word
CD, CU	Counters	Counter Down, Counter Up
S, R	Bit logic instruction	Set, Reset
NOT	Bit logic instruction	Negate RLO
FP	Bit logic instruction	Edge Positive
+I	Floating-Point instruction	Add Accumulators 1 and 2 as Integer
/I	Floating-Point instruction	Divide Accumulator 2 by Accumulator 1 as Integer
*I	Floating-Point instruction	Multiply Accumulators 1 and 2 as Integers
>=I, <=I	Compare	Compare Integer
A, AN	Bit logic instruction	And, And Not
O, ON	Bit logic instruction	Or, Or Not
=	Bit logic instruction	Assign
INC	Accumulator	Increment Accumulator 1
BE, BEC	Program Control	Block End and Block End Conditional
L, T	Load / Transfer	Load and Transfer
SE	Timers	Extended Pulse Timer



System Component	Absolute Address	Symbol	Symbol Table
Push Button Start Switch	I 1.1	S1	I 1.1 S1
Push Button Stop Switch	I 1.2	S2	I 1.2 S2
Push Button Start Switch	I 1.3	S3	I 1.3 S3
Push Button Stop Switch	I 1.4	S4	I 1.4 S4
Sensor	I 1.5	S5	I 1.5 S5
Motor	Q 4.0	MOTOR_ON	Q 4.0 MOTOR_ON

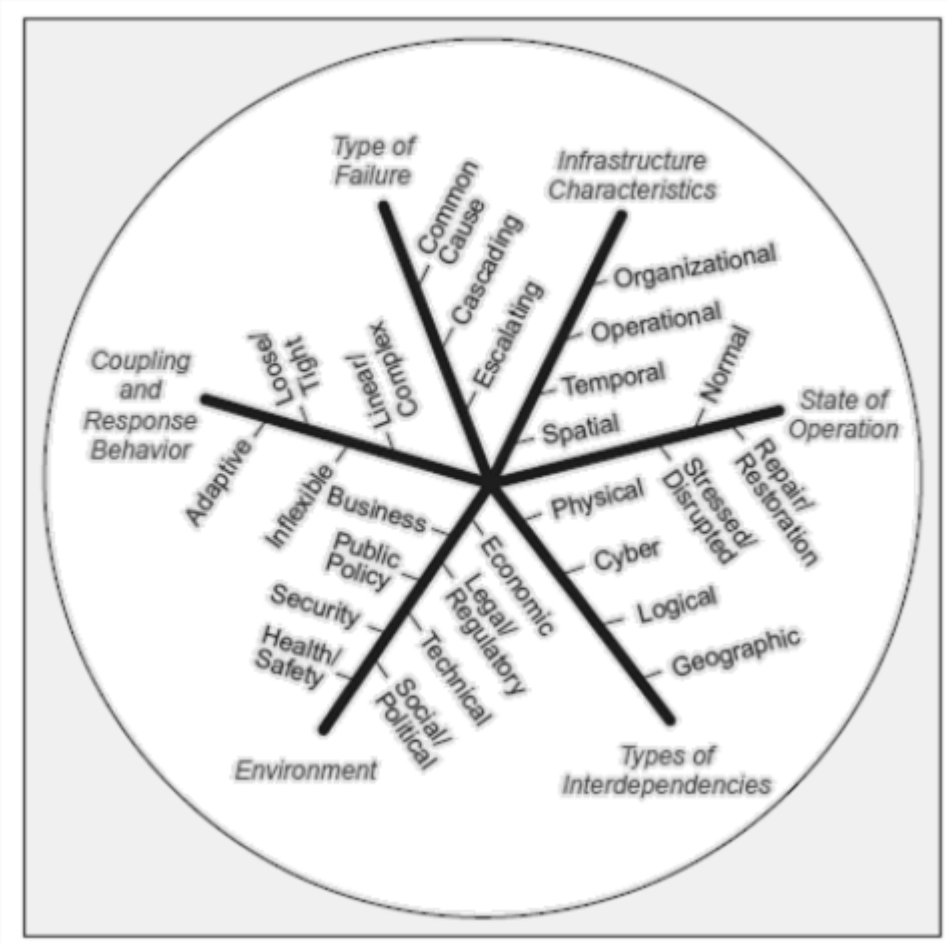
Absolute Program		Symbolic Program	
O	I 1.1	O	S1
O	I 1.3	O	S3
S	Q 4.0	S	MOTOR_ON
O	I 1.2	O	S2
O	I 1.4	O	S4
ON	I 1.5	ON	S5
R	Q 4.0	R	MOTOR_ON

```
STL          Explanation
O    I 1.1   //Pressing either start switch turns the motor on.
O    I 1.3
S    Q 4.0
O    I 1.2   //Pressing either stop switch or opening the normally closed contact at
             //the end of the belt turns the motor off.
O    I 1.4
ON   I 1.5
R    Q 4.0
```

Interdependencies

- Links between SCADA and DCS – for example power generation (DCS) linked with power distribution (SCADA).
- Interdependencies between critical infrastructure sectors – for example water treatment systems reliant on Grid.
- Possibilities of cascading failures.

Interdependencies, contd



From: SM Rinaldi et al: Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems Magazine, 21(6), 2001.

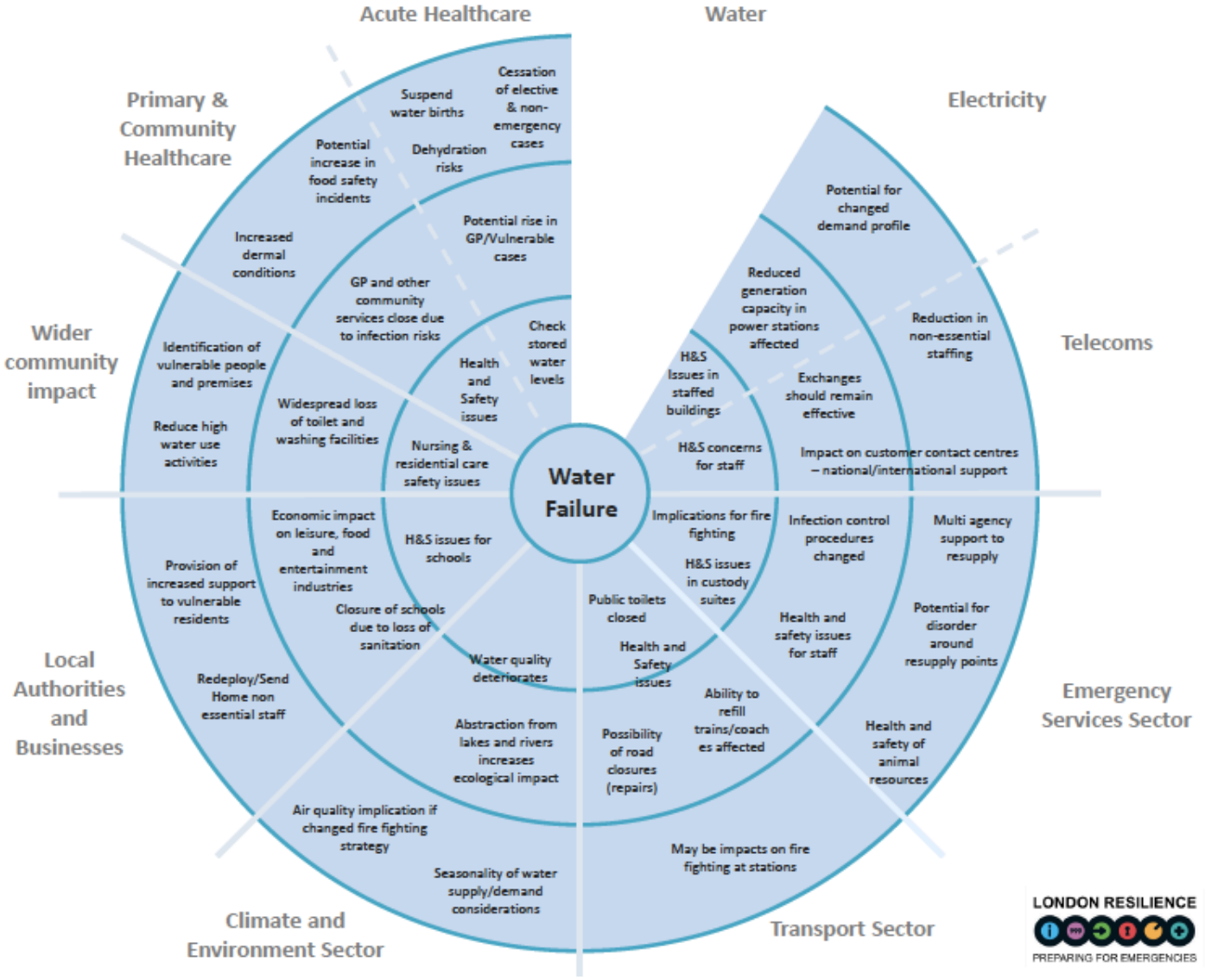
Interdependencies, contd

From: Anytown: Final Report

A DEFRA funded project - Community Resilience Funding for Local Resilience Forums in England

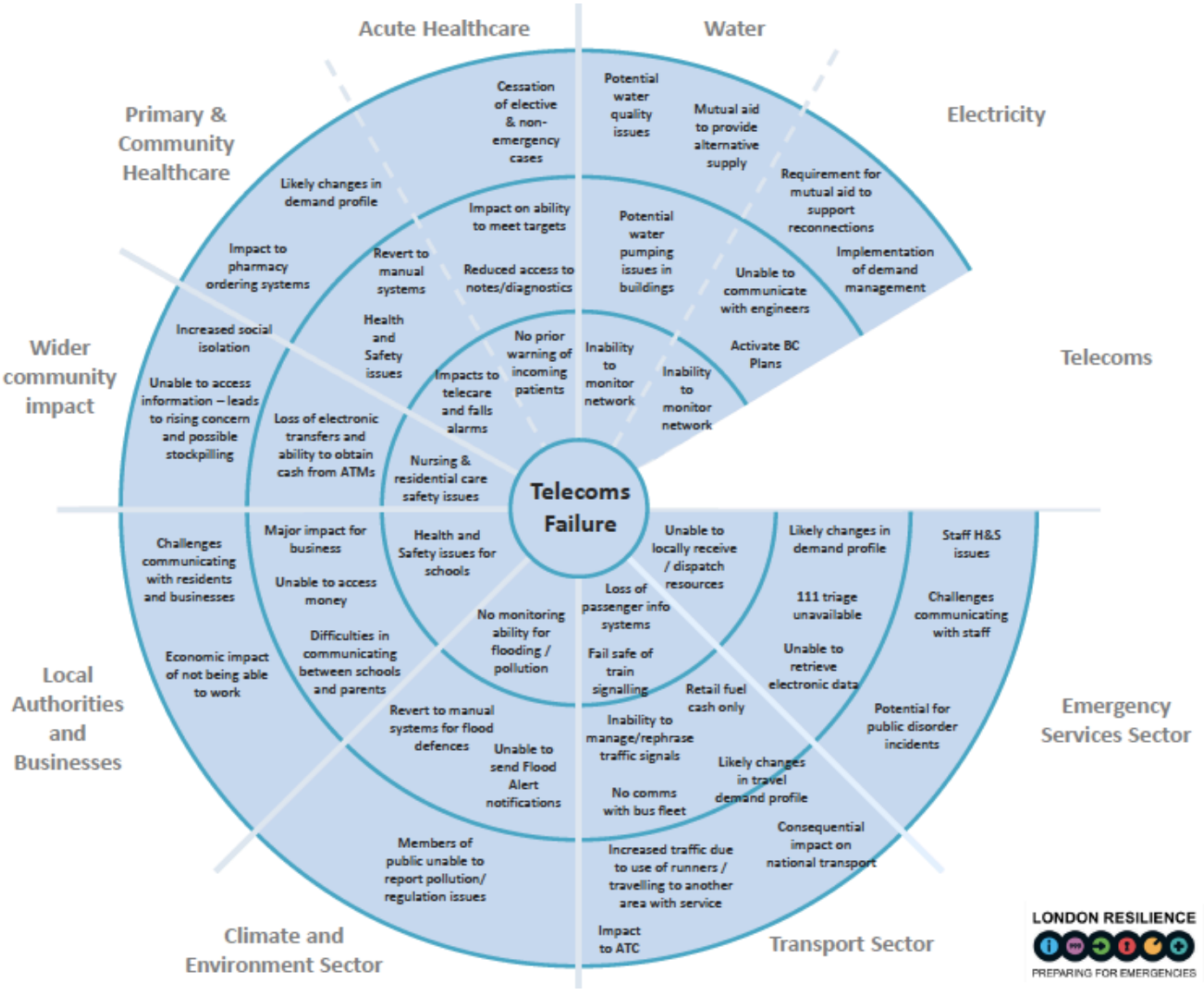
Matthew Hogan, London Resilience Team

Interdependencies, contd



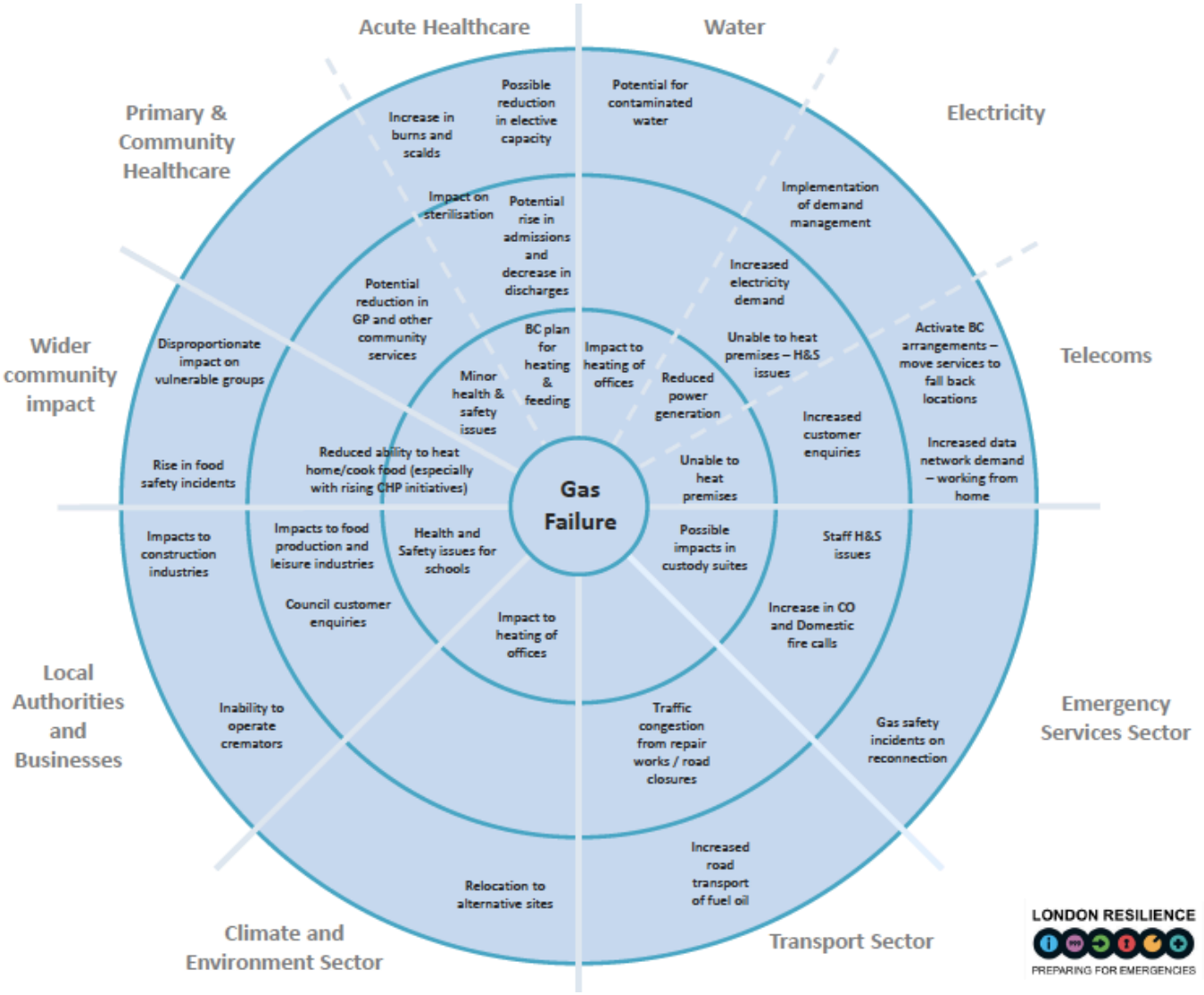
LONDON RESILIENCE
PREPARING FOR EMERGENCIES

Interdependencies, contd



LONDON RESILIENCE
PREPARING FOR EMERGENCIES

Interdependencies, contd



LONDON RESILIENCE
PREPARING FOR EMERGENCIES

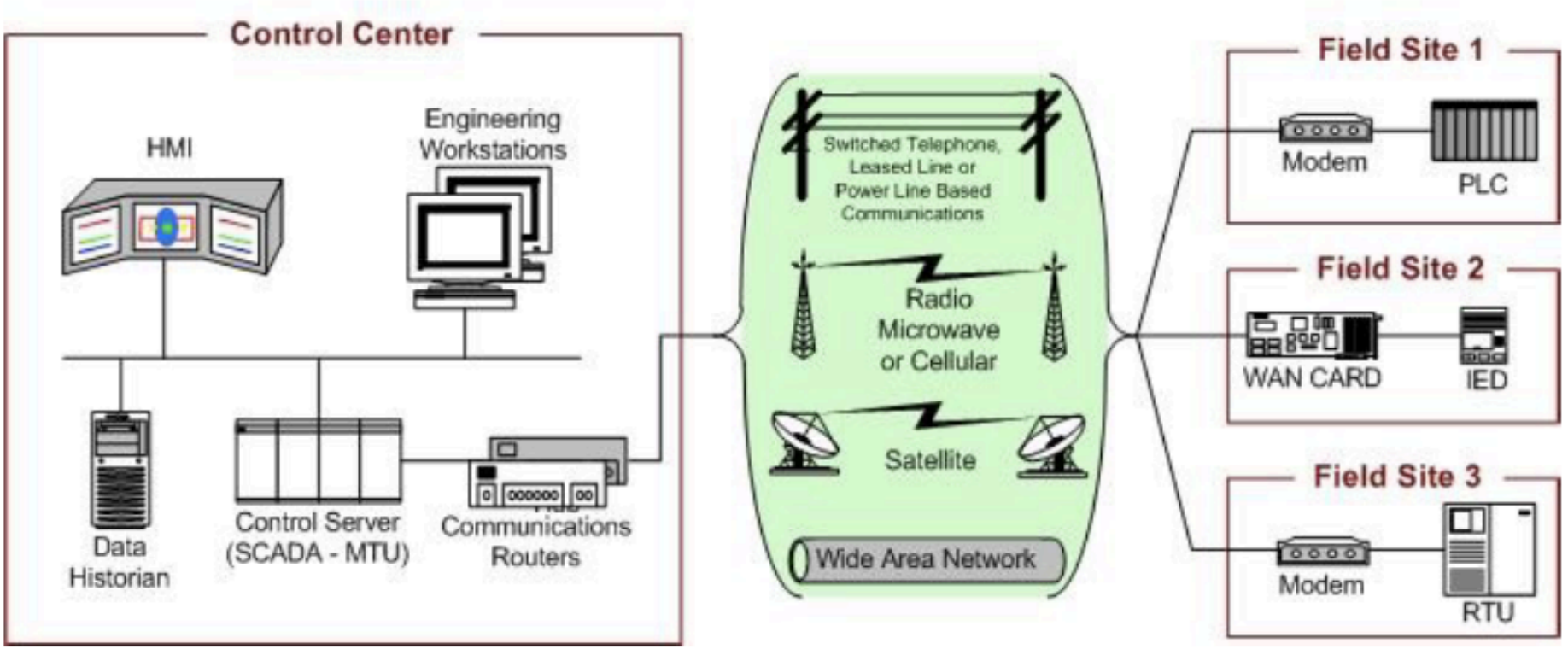
UK Power Outage, August 2019

- Lightning strike on transmission circuit at 4.52pm on Friday 9 August – return to normal operation after 20 seconds
- Off-shore windfarm and gas powered station both reduced supply – loss of 5% (1GW) capacity
- 1.1M customers without power for 15-50 minutes
- Trains stopped on SE rail – a number of cases, engineers were required to restart
- Other critical facilities affected – for example Ipswich hospital and Newcastle airport.

ICS Design Considerations

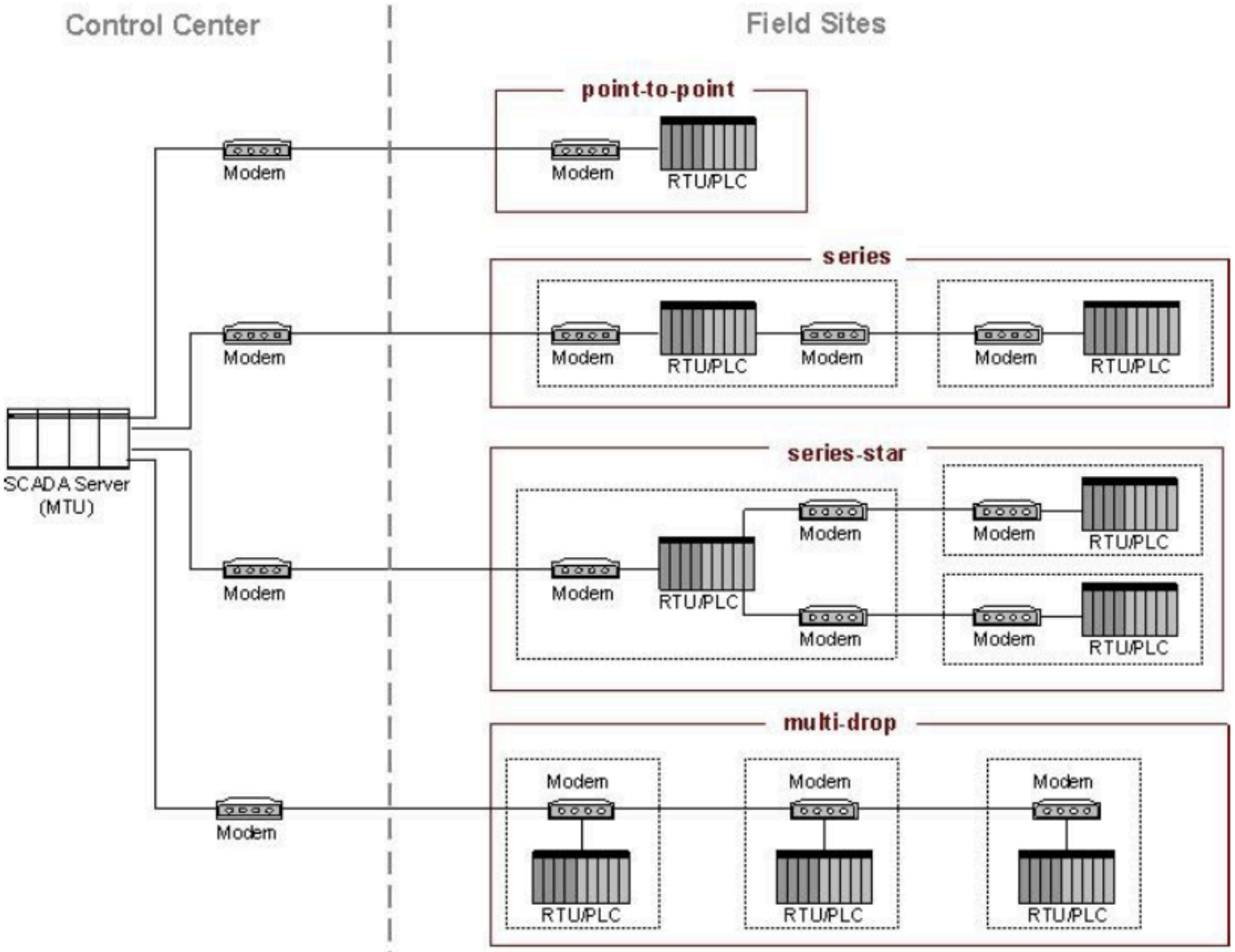
- Control Timing Requirements
- Geographic Distribution
- Hierarchy
- Control Complexity
- Availability
- Impact of Failures
- Safety

SCADA



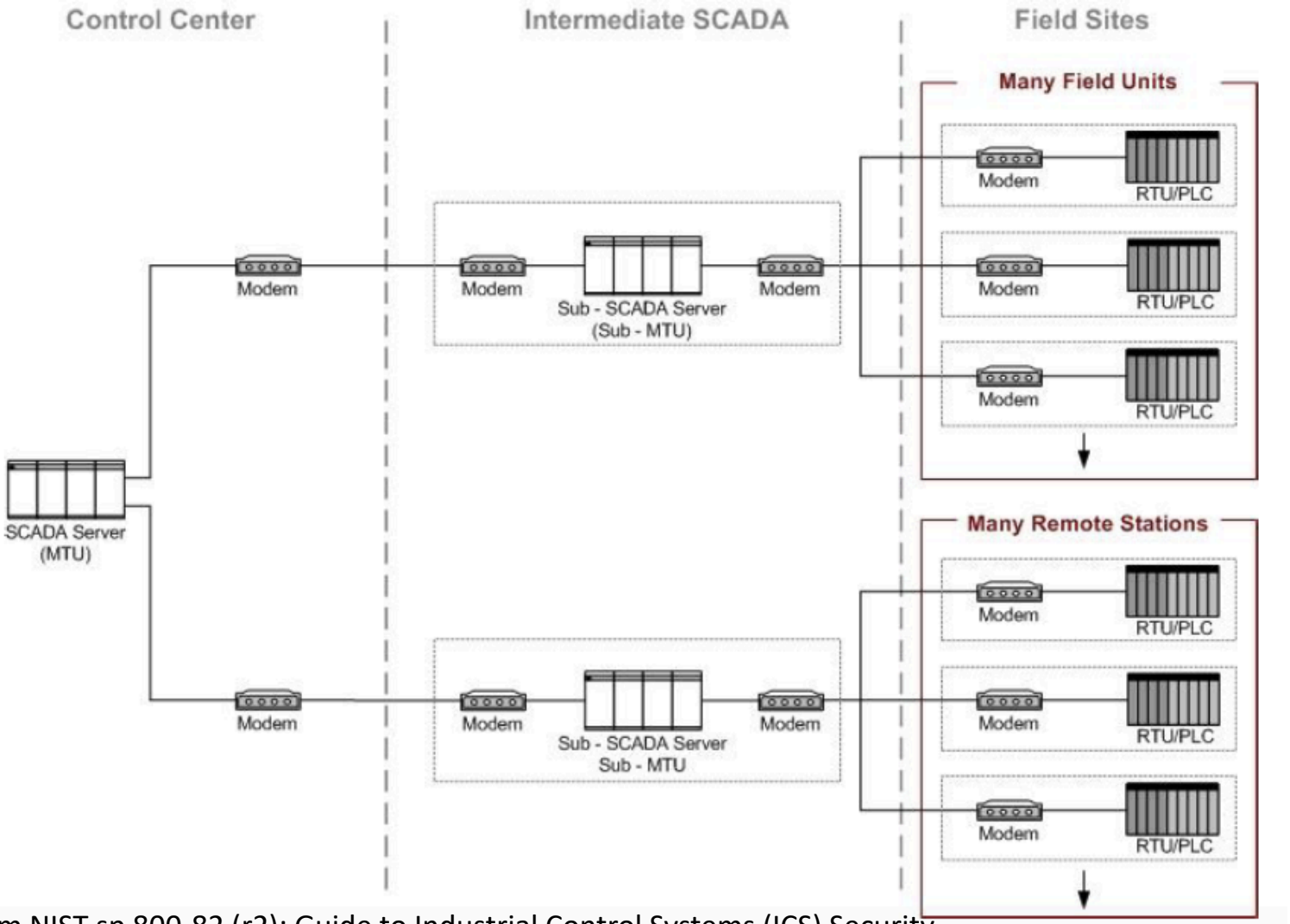
From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security

Basic SCADA Comms Topologies



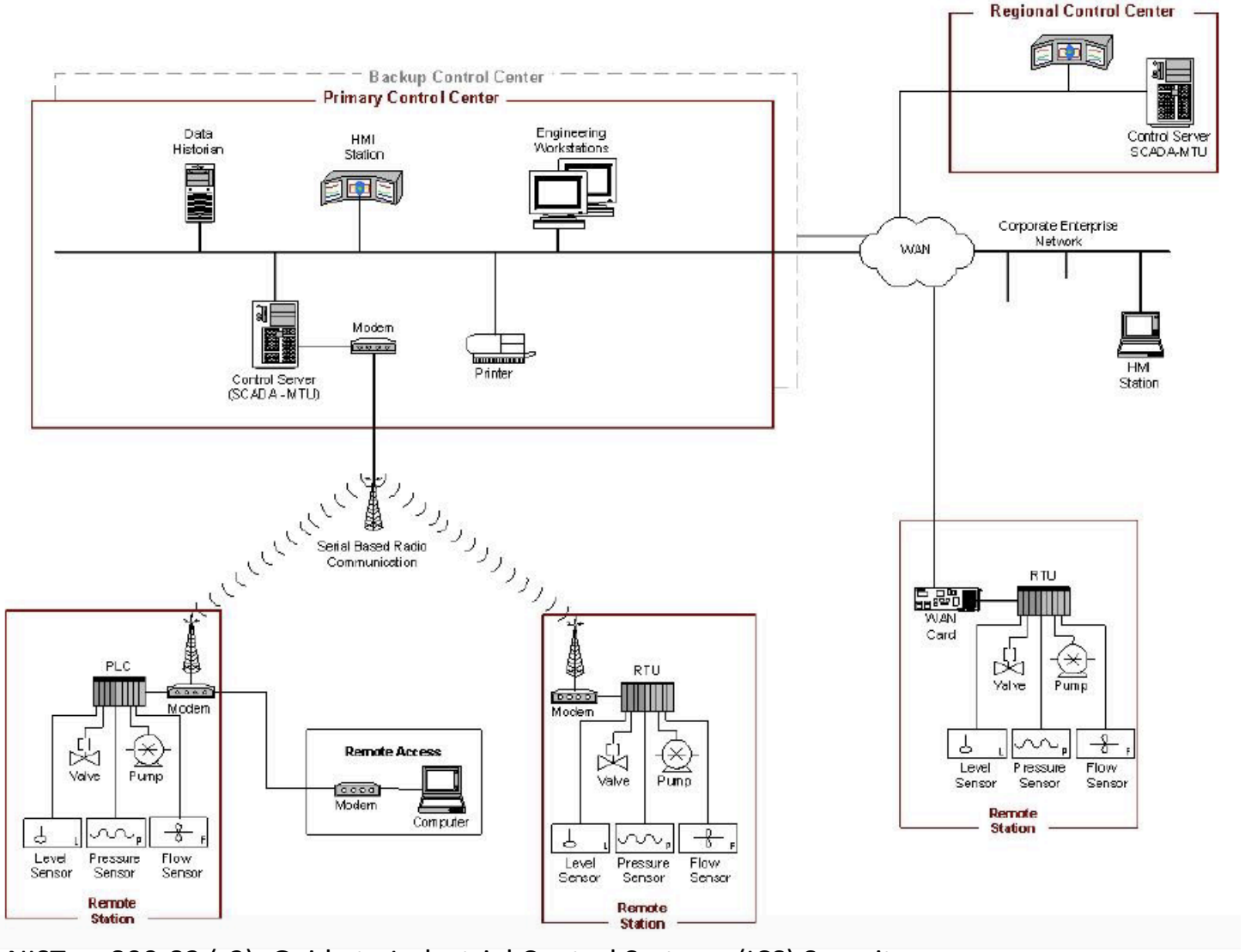
From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security

Large SCADA Comms Topology



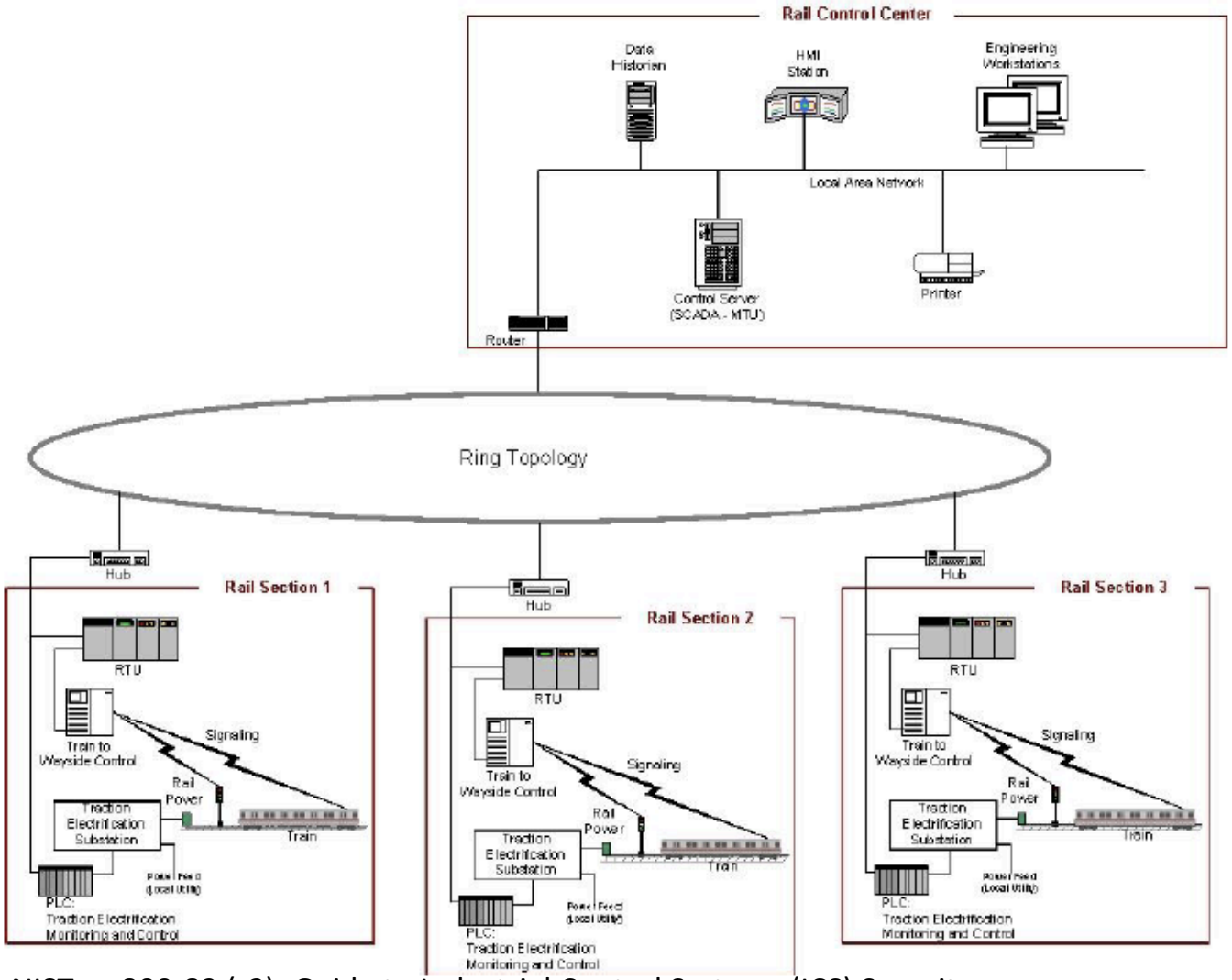
From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security

Example of Implementation



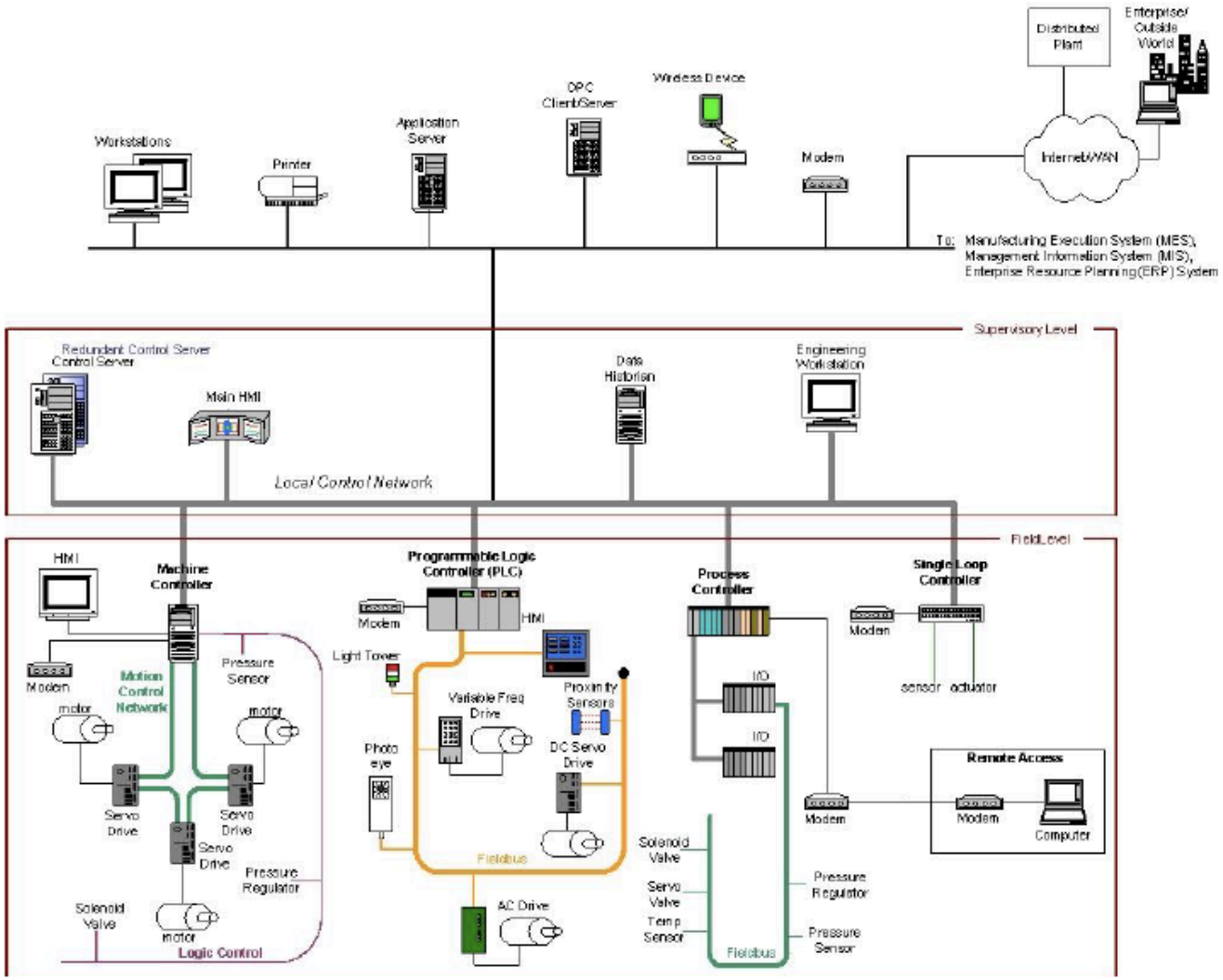
From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security

Rail Monitoring and Control



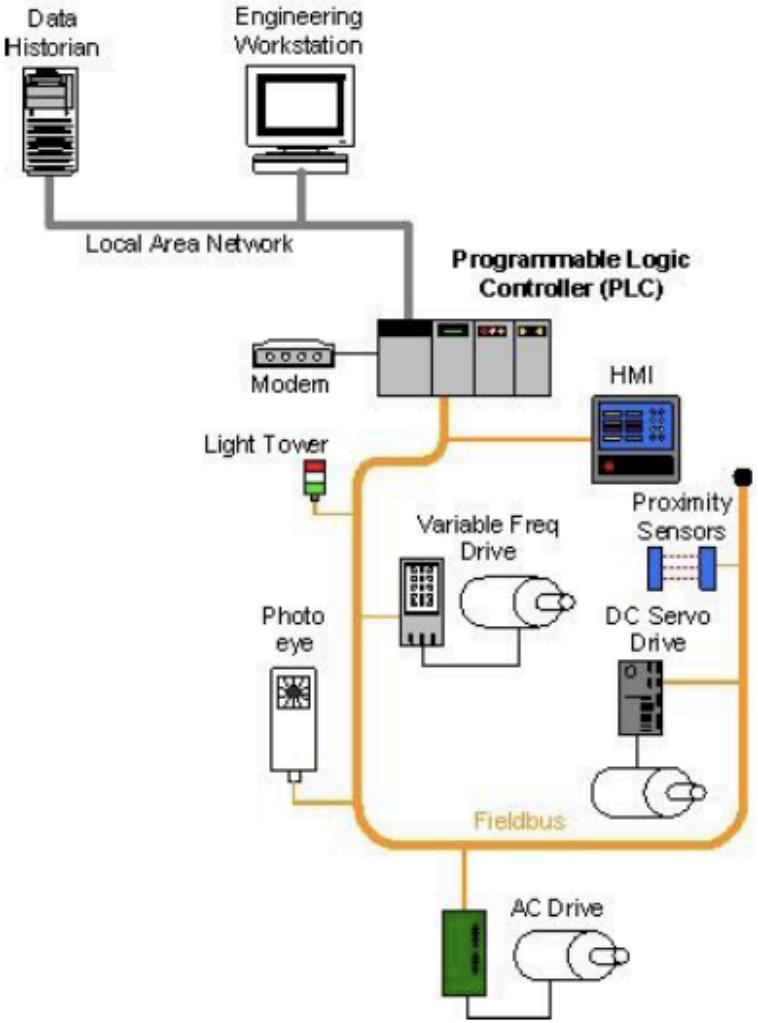
From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security

DCS Implementation



From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security

PLC Control System Example



From NIST sp 800-82 (r2): Guide to Industrial Control Systems (ICS) Security

Modbus TCP/IP

- Protocol Data Unit (PDU) and Application Data Unit (ADU)
- The ADU consists of an Address, PDU and Error Check
- PDU format: Transaction ID, Protocol ID, Length, Unit ID, Function Code, Data
- Read, Write, Diagnostic codes
- Vulnerabilities: Identification, MITM, undocumented Function codes

Ethernet/IP

- Built on Common Industrial Protocol (CIP)
- CIP packet structure: Command, Length, Session handle, Status, Sender context, Options, Command specific data
- Vulnerabilities: Identification, MITM, undocumented commands

DNP3

- Distributed Network Protocol
- Data Link Layer – source and destination
- Transport Control Layer – fragmented packets sequence
- Application Layer – Function codes
- Read, Write, Delete, Restart
- Vulnerabilities: Identification, Fuzzing

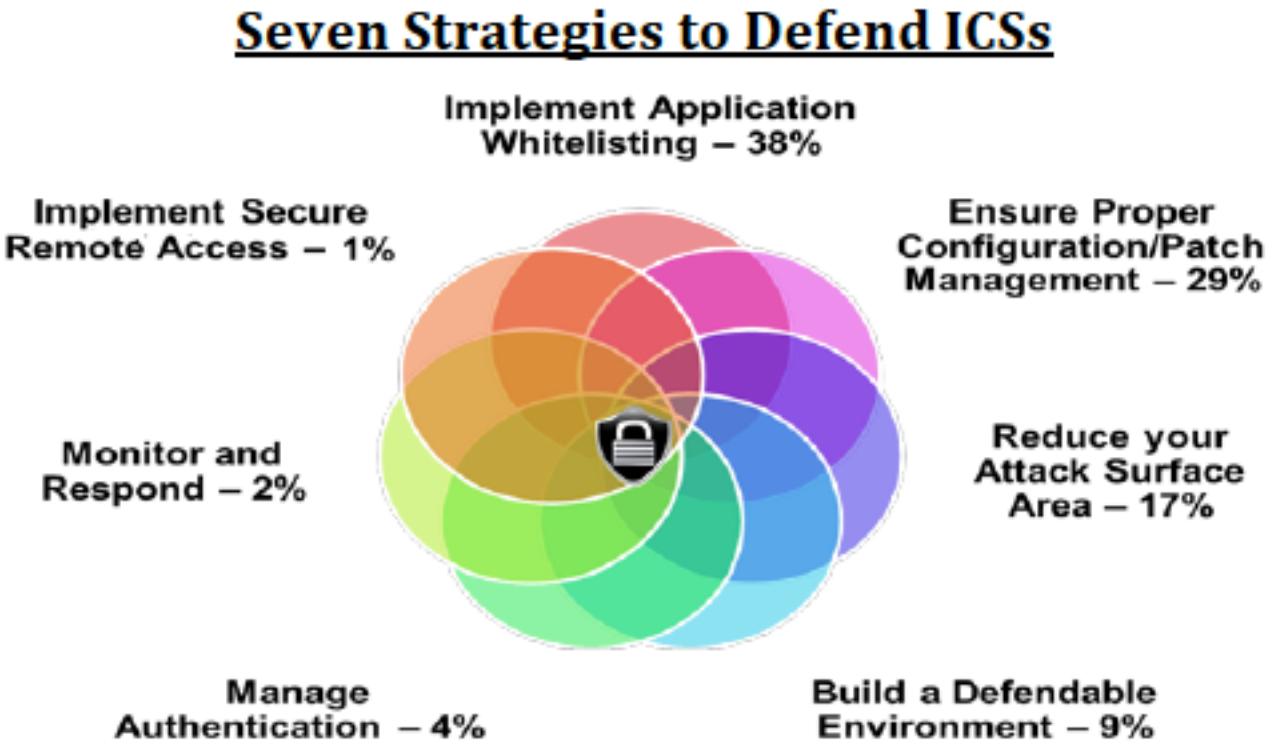
Siemens S7comms

- Proprietary protocol
- S7 STP CPU
- S7 Identification
- S7 Password Brute Force

Countermeasures

- Keep firmware up to date
- Strong Network Segmentation and Network Security
- Password Brute-Force Countermeasures to prevent attacker from being able to gain access to password files

ICS-CERT Advice (based on 2013/2014)



INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM