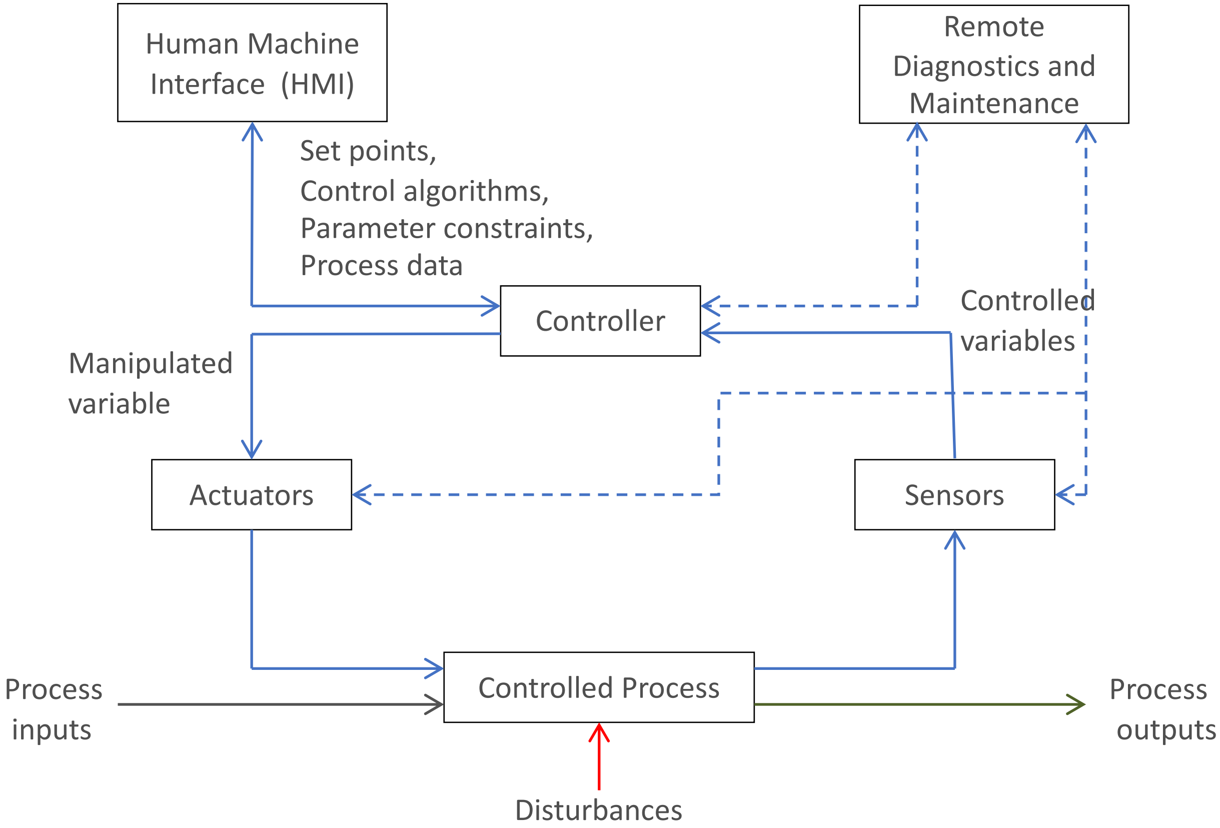
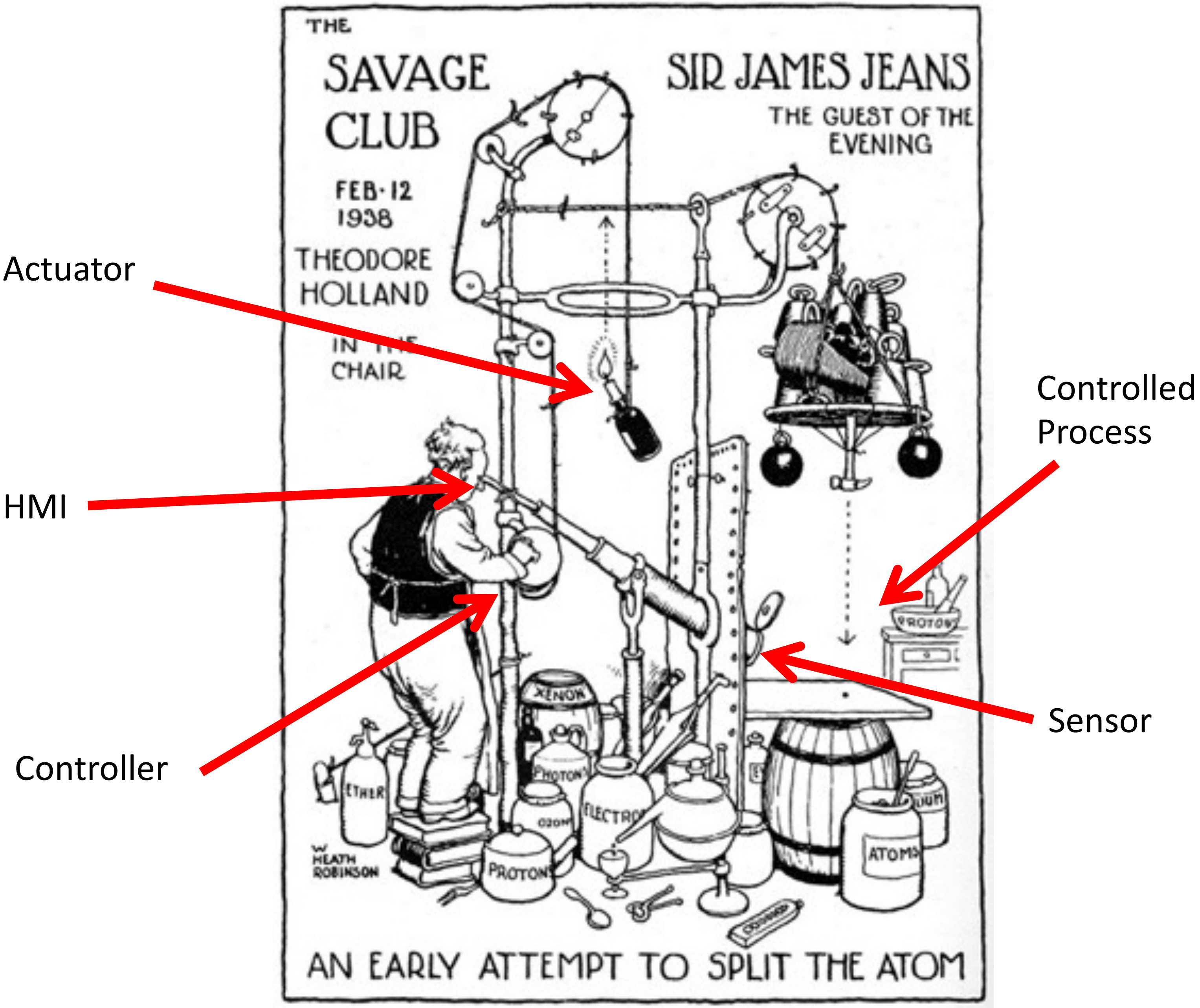
Industrial Control Systems

Chris Hankin

Generic ICS Architecture





Actuator

HMI

Controller

Controlled Process

Sensor

Credit: William Heath Robinson Trust

Glossary

- DCS: Distributed Control System – intelligence gathering throughout controlled process
- IED: Intelligent Electronic Device – I/O capability
- PLC: Programmable Logic Controller – User programmable
- 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

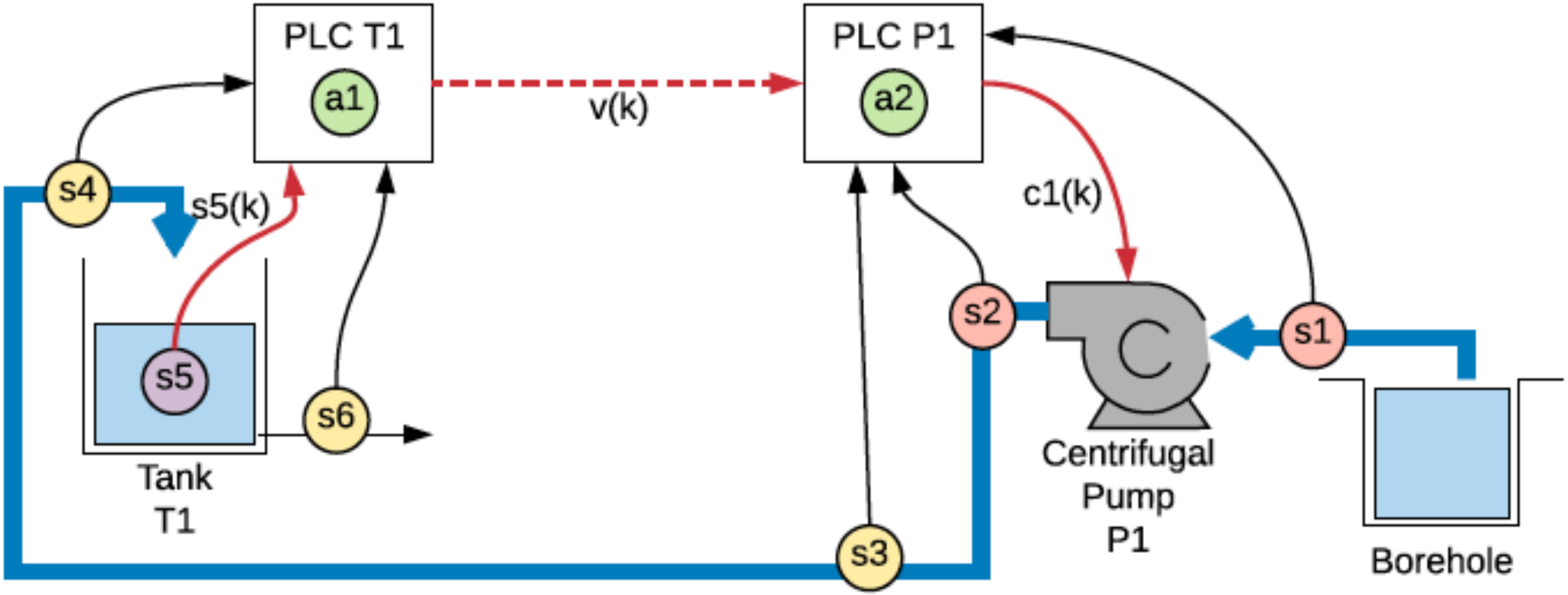
Control Components

- 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

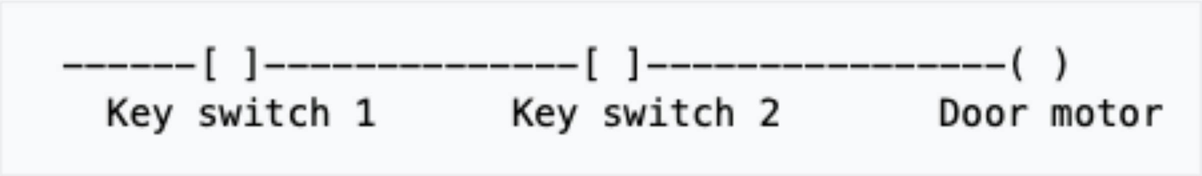
- Manufacturing
    - Process-based:
        - Continuous Processes – for example, petroleum in a refinery or distillation in a chemical plant.
        - Batch Manufacturing – distinct start and end point, for example in food production.
    - Discrete: parts assembly and machining
- Distribution industries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

Water Distribution



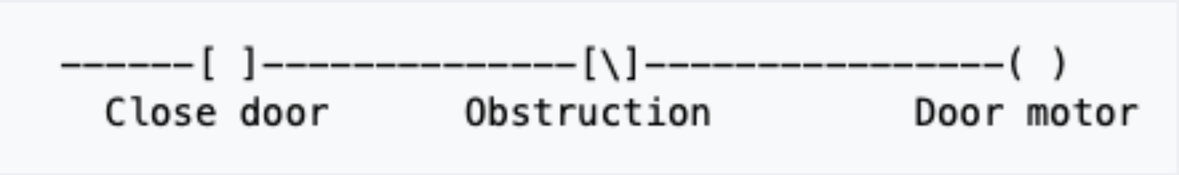
Ladder Logic (Wikipedia)

AND



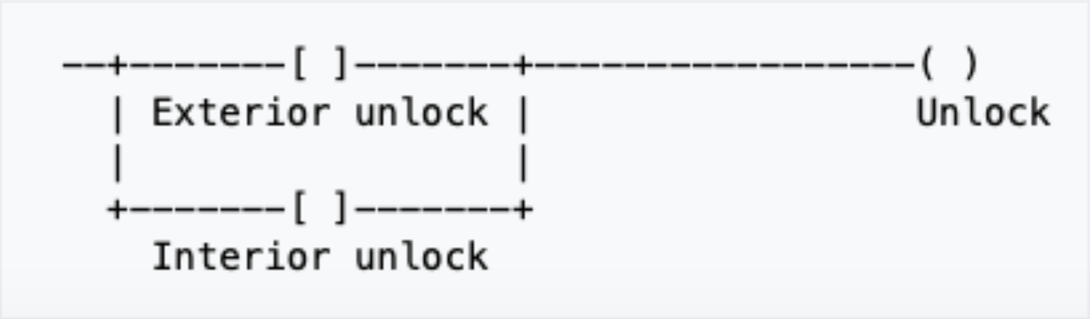
```
------[ ]--------------[ ]----------------( )
  Key switch 1      Key switch 2       Door motor
```

NOT



```
------[ ]--------------[\]----------------( )
  Close door      Obstruction         Door motor
```

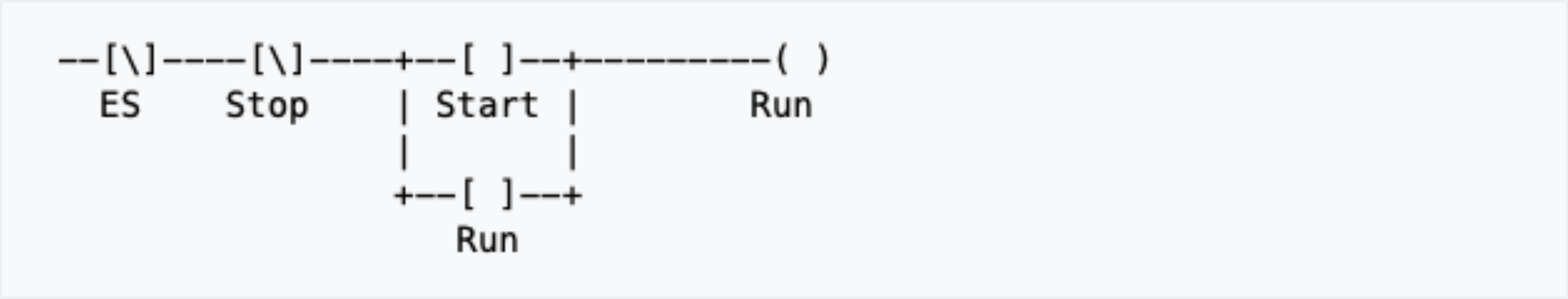
OR



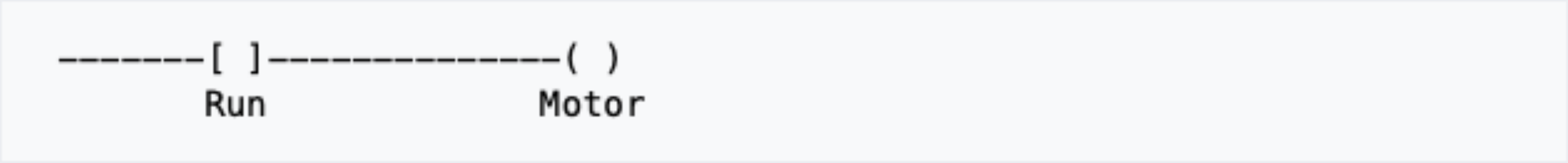
```
--+-------[ ]-------+-----------------( )
  | Exterior unlock |                 Unlock
  |                 |
  +-------[ ]-------+
    Interior unlock
```

[ ] input   ( ) output

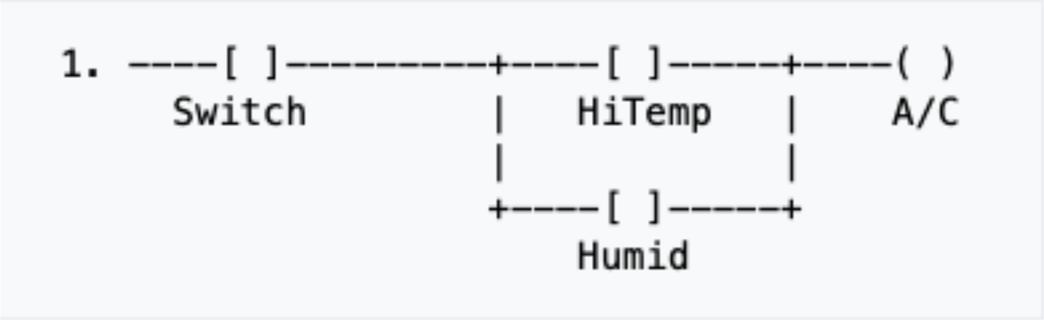
Continued



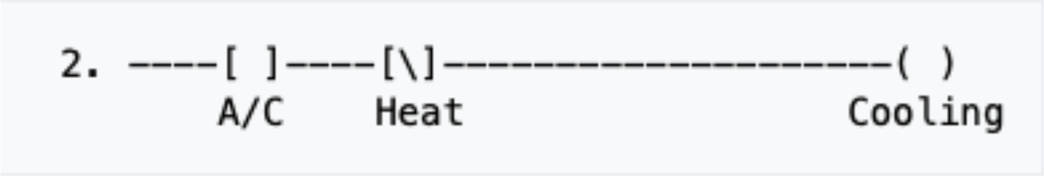
```
--[\]----[\]----+--[ ]--+---------( )
  ES    Stop    | Start |       Run
                |       |
                +--[ ]--+
                   Run
```



```
-------[ ]--------------( )
       Run              Motor
```

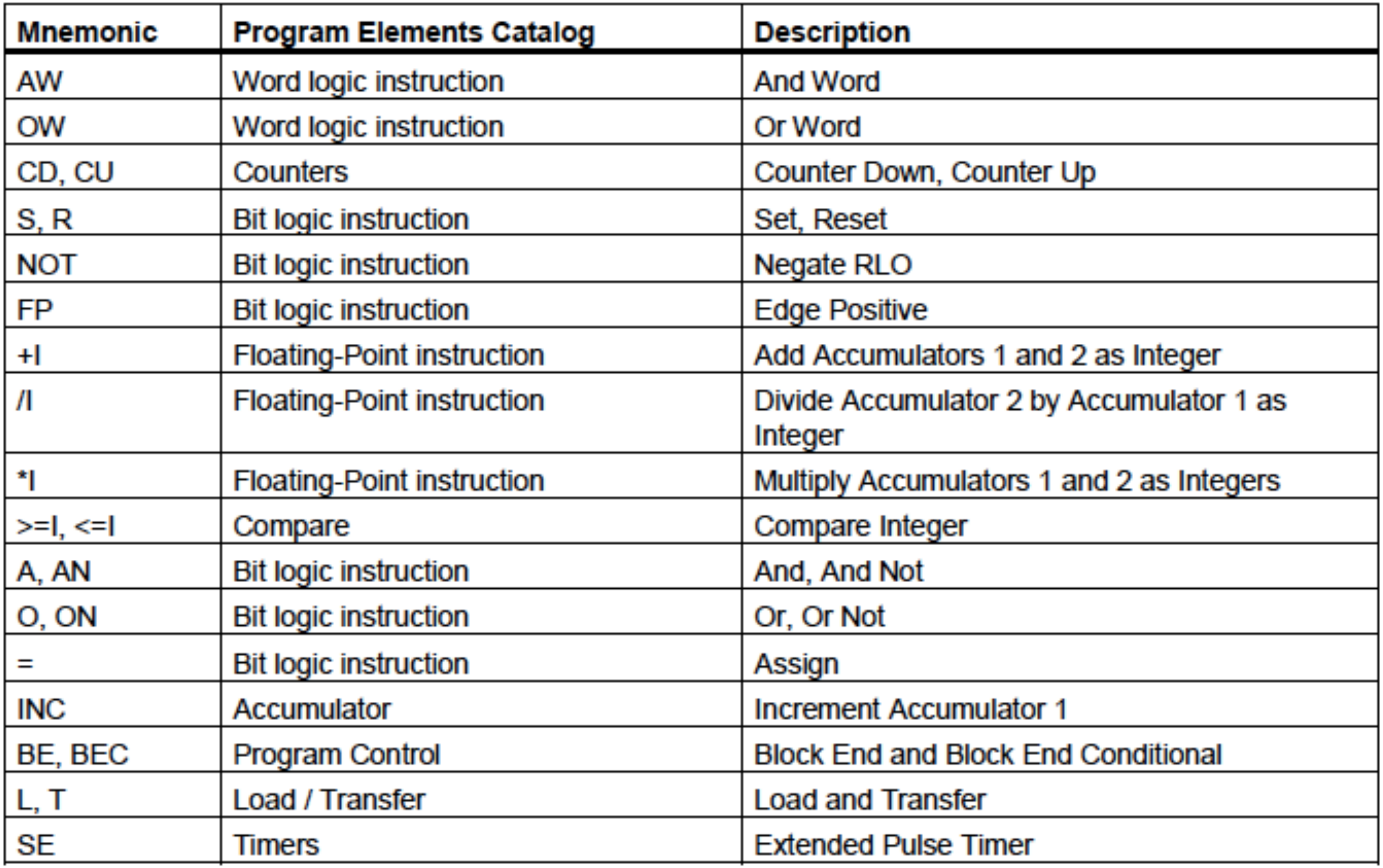


```
1. ----[ ]---------+----[ ]-----+----( )
     Switch        |   HiTemp   |    A/C
                   |            |
                   +----[ ]-----+
                       Humid
```

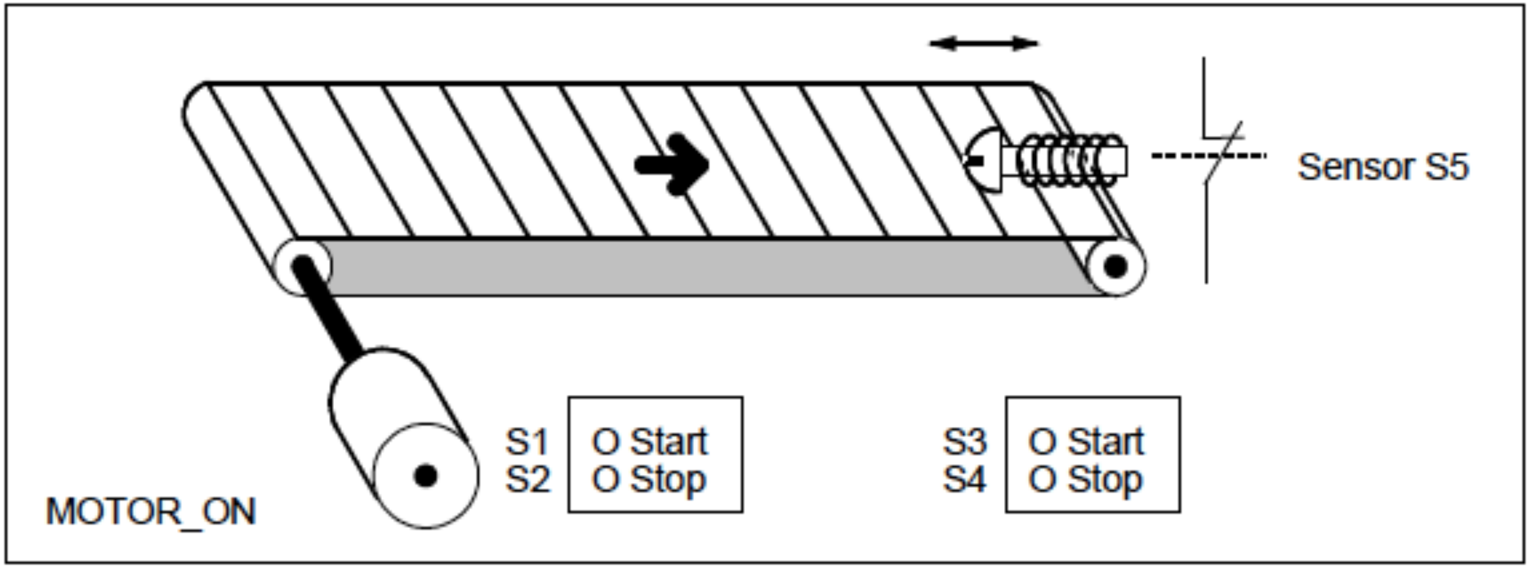


```
2. ----[ ]----[\]--------------------( )
       A/C    Heat                 Cooling
```

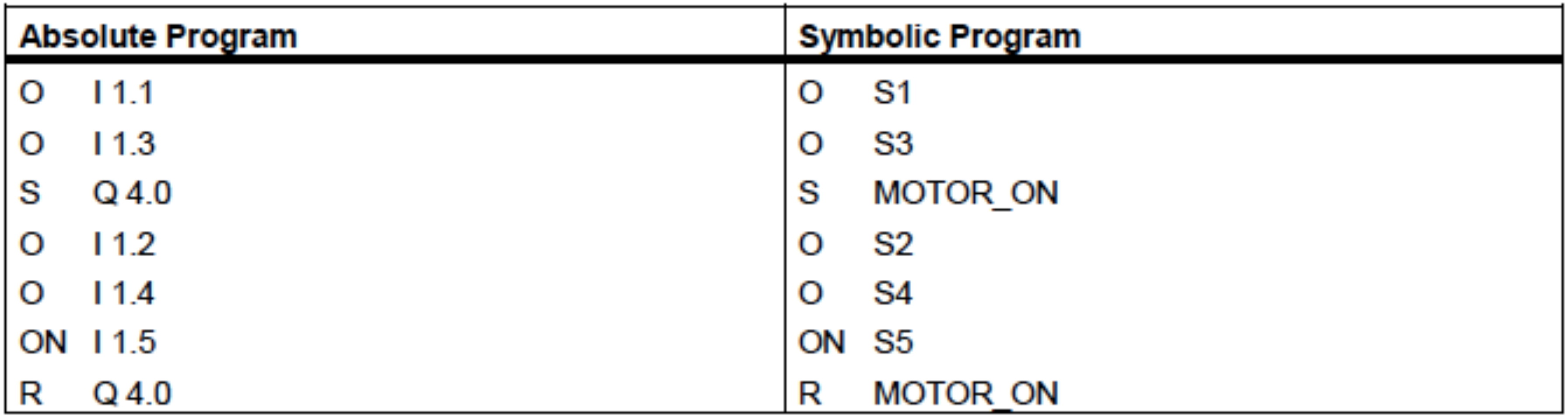
Siemens Step 7



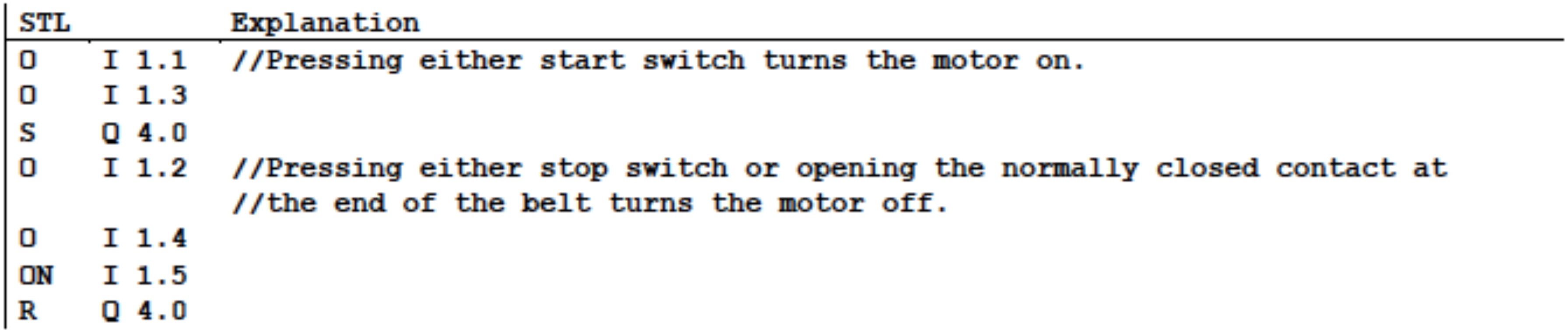
Mnemonic	Program Elements Catalog	Description
AW	Word logic instruction	And Word
OW	Word logic instruction	Or Word
CD, CU	Counters	Counter Down, Counter Up
S, R	Bit logic instruction	Set, Reset
NOT	Bit logic instruction	Negate RLO
FP	Bit logic instruction	Edge Positive
+I	Floating-Point instruction	Add 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

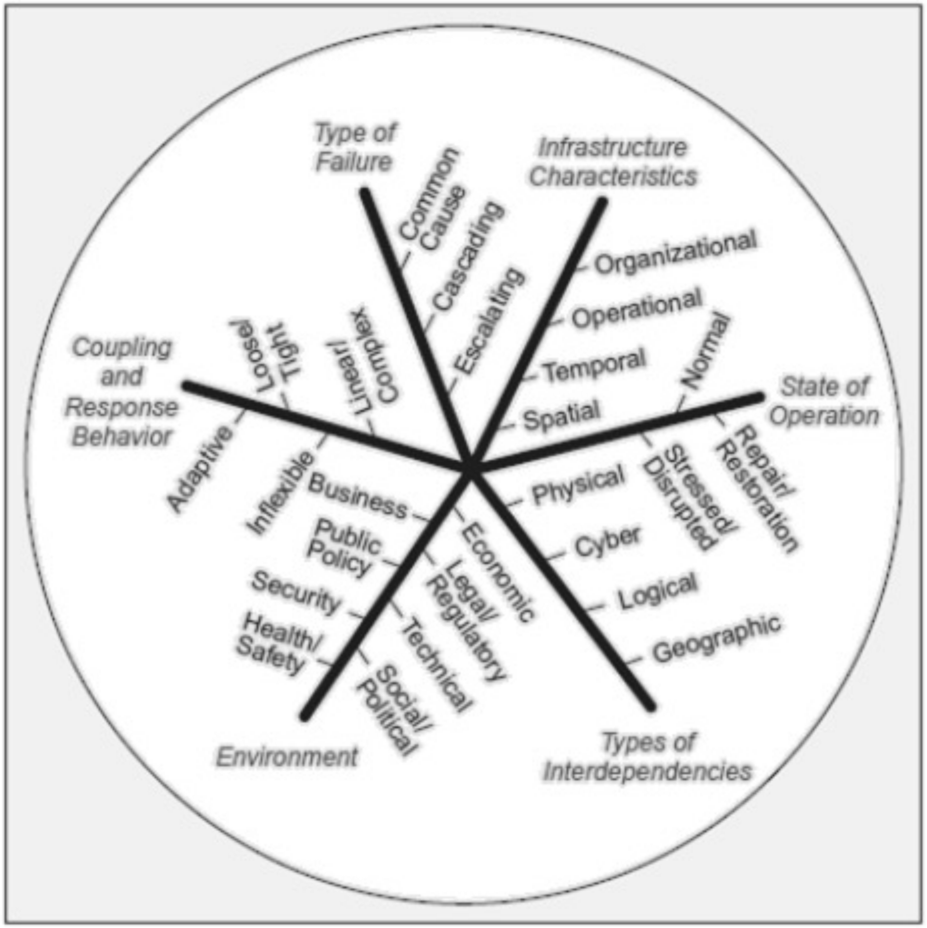


```
STL          Explanation
O    I 1.1   //Pressing either start switch turns the motor on.
O    I 1.3
S    Q 4.0
O    I 1.2   //Pressing either stop switch or opening the normally closed contact at
             //the end of the belt turns the motor off.
O    I 1.4
ON   I 1.5
R    Q 4.0
```

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

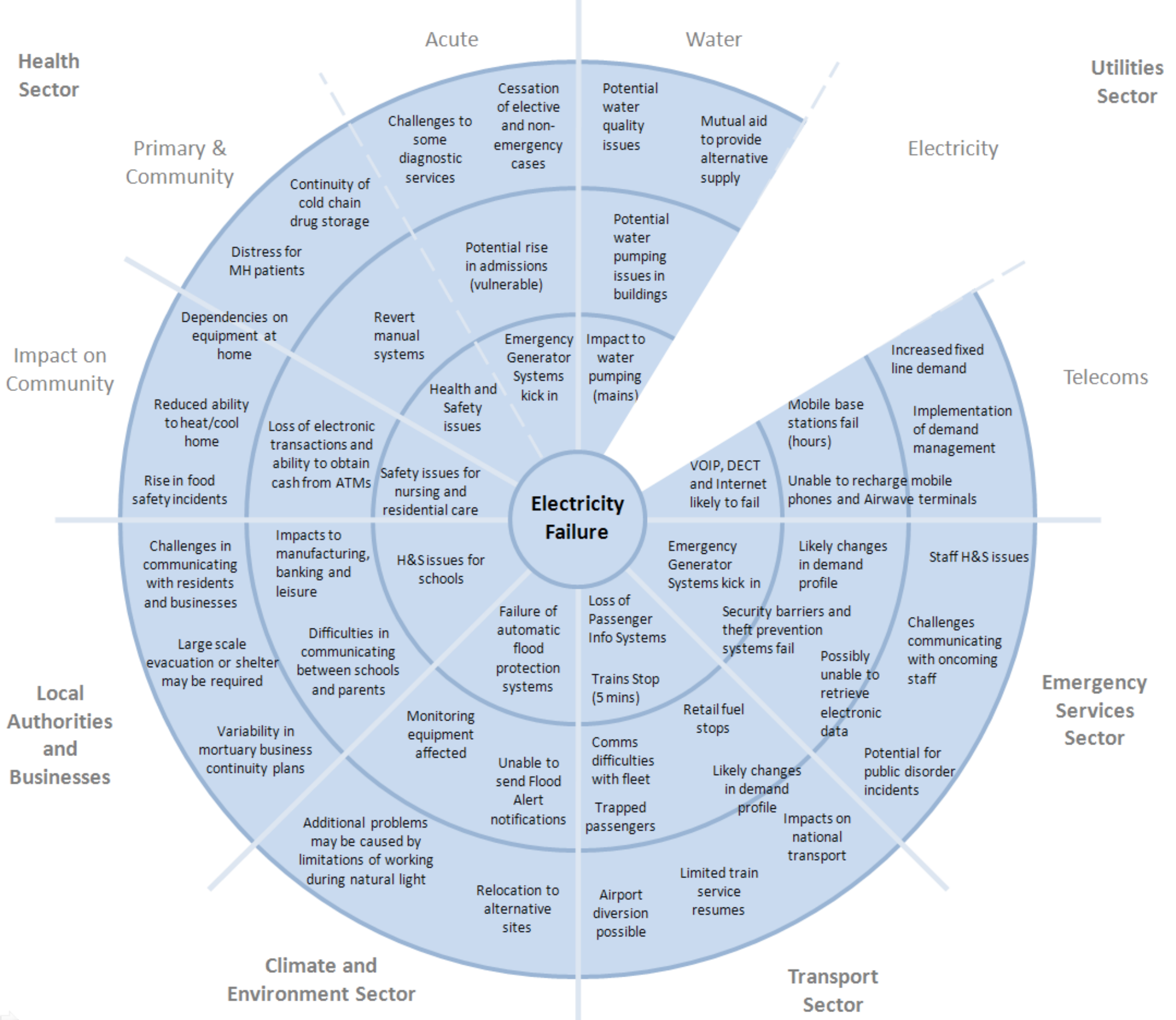


From: SM Rinaldi et al: Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems Magazine, 21(6), 2001.

Interdependencies

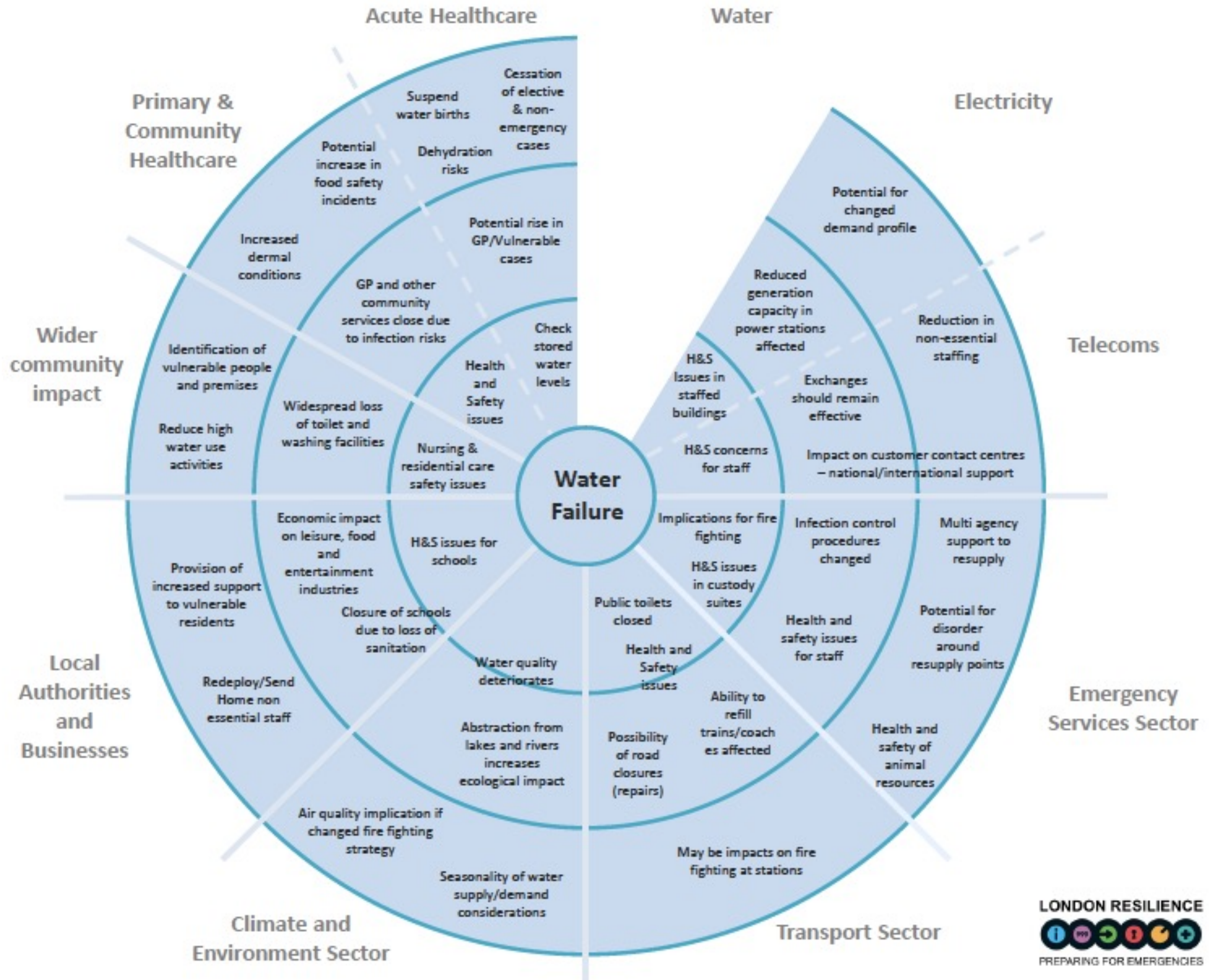
- Physical – rail and coal-fired generation
- Cyber – SCADA and controlled system
- Logical – not physical, cyber or geographic; for example electricity distribution and finance sector
- Geographic – interdepence as a result of proximity

Interdependencies, contd


Electricity Failure
Health Sector
Acute
Primary & Community
Cessation of elective and non-emergency cases
Challenges to some diagnostic services
Continuity of cold chain drug storage
Distress for MH patients
Potential rise in admissions (vulnerable)
Revert manual systems
Emergency Generator Systems kick in
Health and Safety issues
Utilities Sector
Water
Electricity
Potential water quality issues
Mutual aid to provide alternative supply
Potential water pumping issues in buildings
Impact to water pumping (mains)
Telecoms
Increased fixed line demand
Implementation of demand management
Mobile base stations fail (hours)
Unable to recharge mobile phones and Airwave terminals
VOIP, DECT and Internet likely to fail
Emergency Services Sector
Emergency Generator Systems kick in
Likely changes in demand profile
Staff H&S issues
Security barriers and theft prevention systems fail
Challenges communicating with oncoming staff
Possibly unable to retrieve electronic data
Retail fuel stops
Potential for public disorder incidents
Transport Sector
Loss of Passenger Info Systems
Trains Stop (5 mins)
Comms difficulties with fleet
Trapped passengers
Likely changes in demand profile
Impacts on national transport
Limited train service resumes
Airport diversion possible
Climate and Environment Sector
Failure of automatic flood protection systems
Monitoring equipment affected
Unable to send Flood Alert notifications
Relocation to alternative sites
Additional problems may be caused by limitations of working during natural light
Local Authorities and Businesses
H&S issues for schools
Impacts to manufacturing, banking and leisure
Difficulties in communicating between schools and parents
Challenges in communicating with residents and businesses
Large scale evacuation or shelter may be required
Variability in mortuary business continuity plans
Impact on Community
Safety issues for nursing and residential care
Loss of electronic transactions and ability to obtain cash from ATMs
Dependencies on equipment at home
Reduced ability to heat/cool home
Rise in food safety incidents

From: Anytown: Final Report
A DEFRA funded project - Community Resilience Funding for Local Resilience Forums in England
Matthew Hogan, London Resilience Team

Interdependencies, contd



Water Failure

Acute Healthcare

Cessation of elective & non-emergency cases

Suspend water births

Dehydration risks

Potential rise in GP/Vulnerable cases

Check stored water levels

Primary & Community Healthcare

Potential increase in food safety incidents

GP and other community services close due to infection risks

Health and Safety issues

Wider community impact

Increased dermal conditions

Identification of vulnerable people and premises

Reduce high water use activities

Widespread loss of toilet and washing facilities

Nursing & residential care safety issues

Local Authorities and Businesses

Provision of increased support to vulnerable residents

Redeploy/Send Home non essential staff

Economic impact on leisure, food and entertainment industries

Closure of schools due to loss of sanitation

H&S issues for schools

Climate and Environment Sector

Air quality implication if changed fire fighting strategy

Seasonality of water supply/demand considerations

Abstraction from lakes and rivers increases ecological impact

Water quality deteriorates

Transport Sector

May be impacts on fire fighting at stations

Possibility of road closures (repairs)

Ability to refill trains/coaches affected

Public toilets closed

Health and Safety issues

Emergency Services Sector

Health and safety of animal resources

Potential for disorder around resupply points

Multi agency support to resupply

Health and safety issues for staff

Infection control procedures changed

H&S issues in custody suites

Implications for fire fighting

Telecoms

Reduction in non-essential staffing

Impact on customer contact centres – national/international support

Exchanges should remain effective

H&S concerns for staff

Electricity

Potential for changed demand profile

Reduced generation capacity in power stations affected

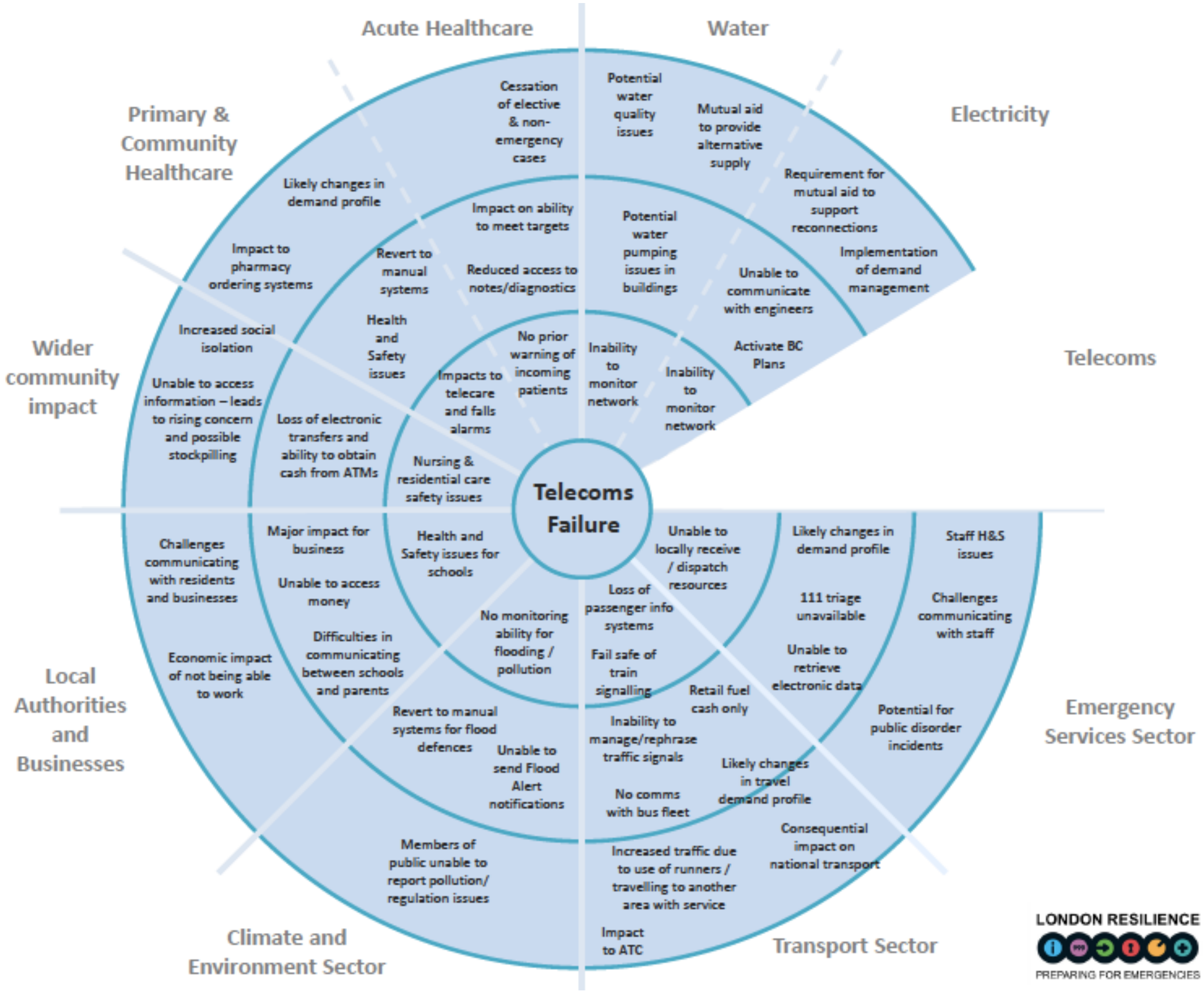
H&S Issues in staffed buildings

Water

LONDON RESILIENCE

PREPARING FOR EMERGENCIES

Interdependencies, contd



Telecoms Failure

Acute Healthcare

Cessation of elective & non-emergency cases

Impact on ability to meet targets

Reduced access to notes/diagnostics

No prior warning of incoming patients

Water

Potential water quality issues

Mutual aid to provide alternative supply

Potential water pumping issues in buildings

Inability to monitor network

Electricity

Requirement for mutual aid to support reconnections

Implementation of demand management

Unable to communicate with engineers

Activate BC Plans

Inability to monitor network

Telecoms

Primary & Community Healthcare

Likely changes in demand profile

Impact to pharmacy ordering systems

Revert to manual systems

Health and Safety issues

Impacts to telecare and falls alarms

Wider community impact

Increased social isolation

Unable to access information – leads to rising concern and possible stockpilling

Loss of electronic transfers and ability to obtain cash from ATMs

Nursing & residential care safety issues

Local Authorities and Businesses

Challenges communicating with residents and businesses

Economic impact of not being able to work

Major impact for business

Unable to access money

Difficulties in communicating between schools and parents

Health and Safety issues for schools

Climate and Environment Sector

Members of public unable to report pollution/ regulation issues

Revert to manual systems for flood defences

Unable to send Flood Alert notifications

No monitoring ability for flooding / pollution

Transport Sector

Loss of passenger info systems

Fail safe of train signalling

Retail fuel cash only

Inability to manage/rephrase traffic signals

No comms with bus fleet

Likely changes in travel demand profile

Increased traffic due to use of runners / travelling to another area with service

Consequential impact on national transport

Impact to ATC

Emergency Services Sector

Unable to locally receive / dispatch resources

Likely changes in demand profile

111 triage unavailable

Unable to retrieve electronic data

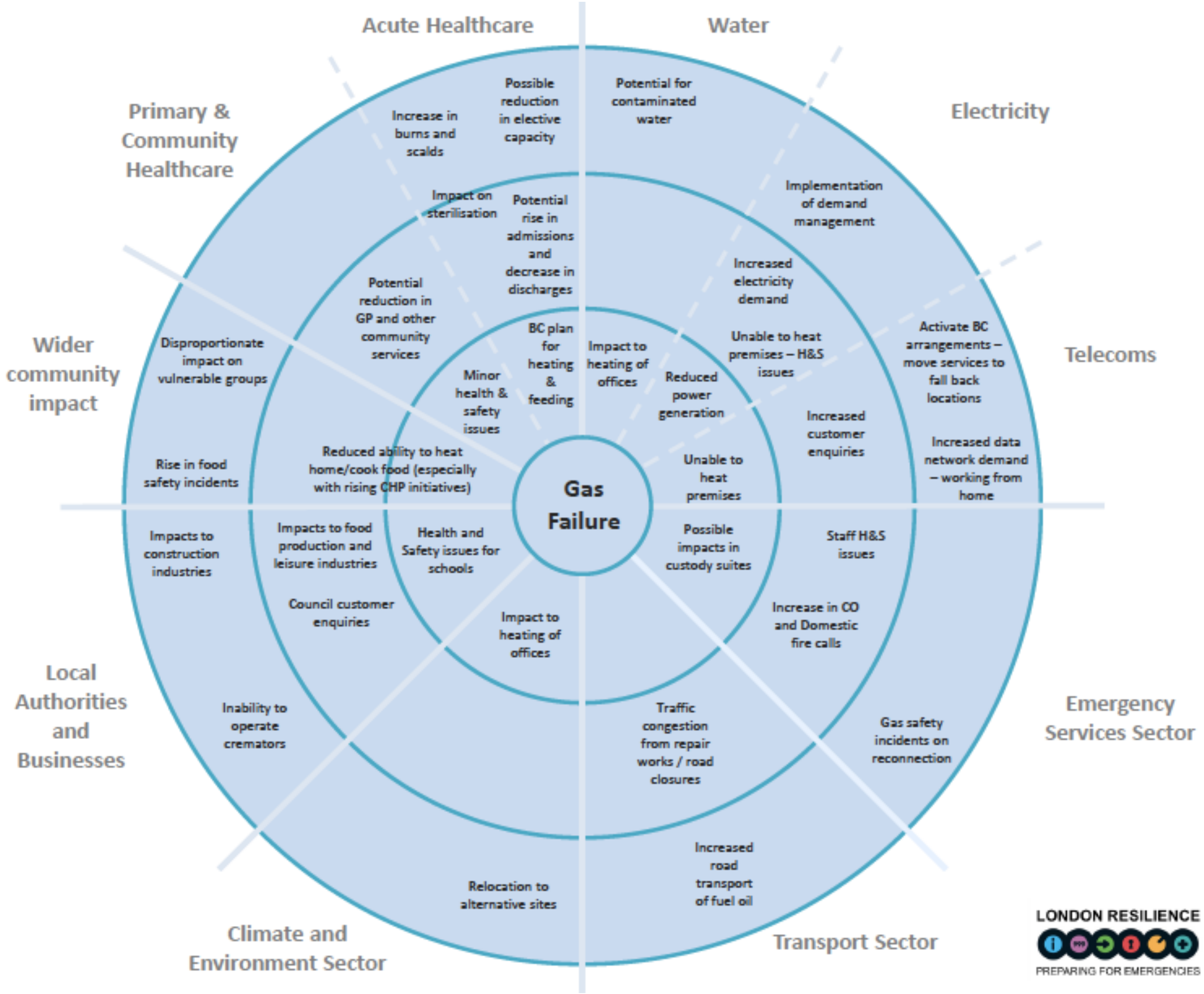
Staff H&S issues

Challenges communicating with staff

Potential for public disorder incidents

LONDON RESILIENCE
PREPARING FOR EMERGENCIES

Interdependencies, contd



Acute Healthcare

Water

Primary & Community Healthcare

Electricity

Increase in burns and scalds

Possible reduction in elective capacity

Potential for contaminated water

Implementation of demand management

Impact on sterilisation

Potential rise in admissions and decrease in discharges

Potential reduction in GP and other community services

Increased electricity demand

Wider community impact

Disproportionate impact on vulnerable groups

BC plan for heating & feeding

Impact to heating of offices

Unable to heat premises – H&S issues

Activate BC arrangements – move services to fall back locations

Telecoms

Minor health & safety issues

Reduced power generation

Increased customer enquiries

Reduced ability to heat home/cook food (especially with rising CHP initiatives)

Rise in food safety incidents

Unable to heat premises

Increased data network demand – working from home

Gas Failure

Impacts to construction industries

Impacts to food production and leisure industries

Health and Safety issues for schools

Possible impacts in custody suites

Staff H&S issues

Council customer enquiries

Impact to heating of offices

Increase in CO and Domestic fire calls

Local Authorities and Businesses

Inability to operate cremators

Traffic congestion from repair works / road closures

Gas safety incidents on reconnection

Emergency Services Sector

Increased road transport of fuel oil

Relocation to alternative sites

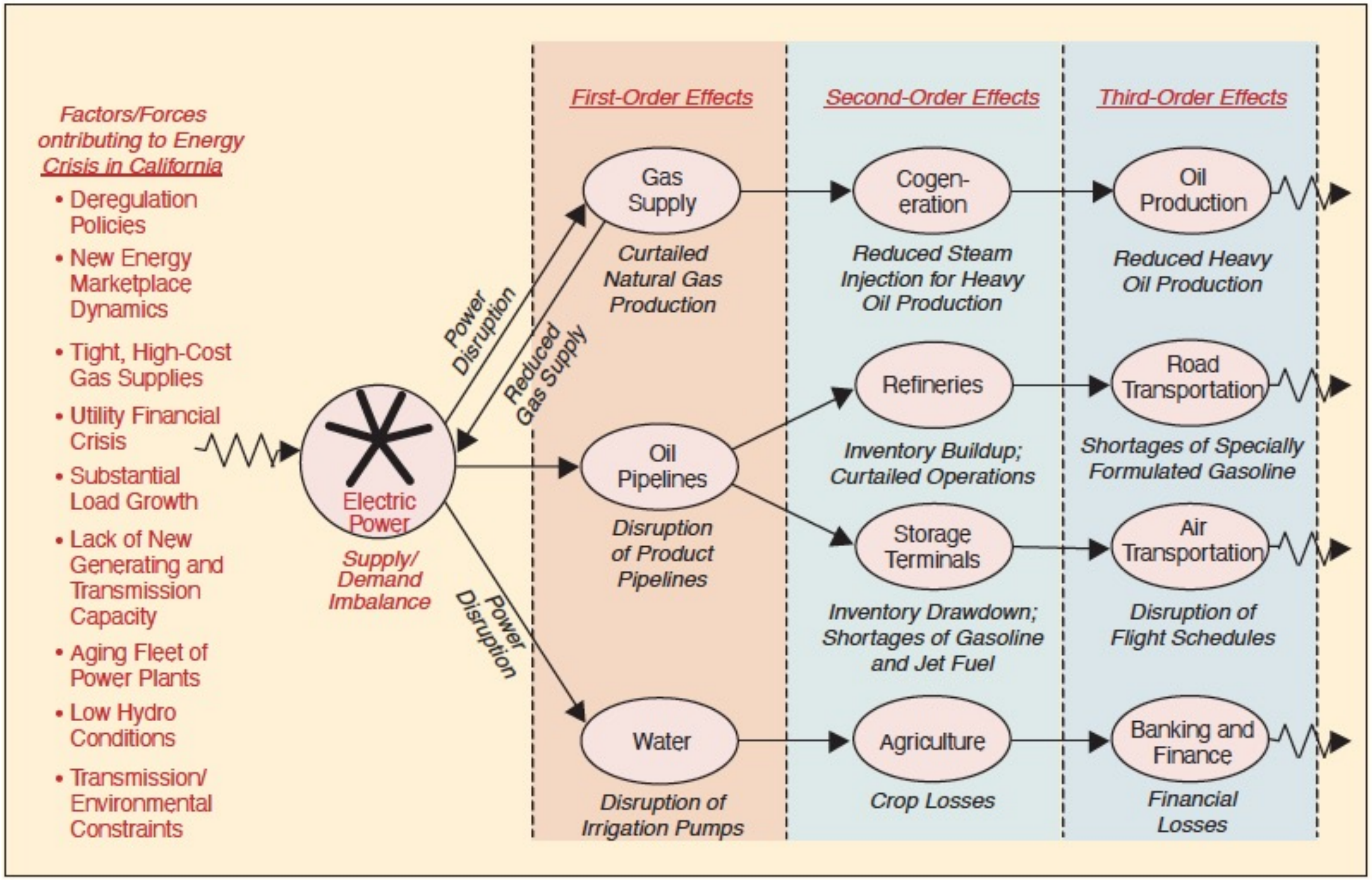
Climate and Environment Sector

Transport Sector

LONDON RESILIENCE

PREPARING FOR EMERGENCIES

Another view:


Factors/Forces ontributing to Energy Crisis in California
• Deregulation Policies
• New Energy Marketplace Dynamics
• Tight, High-Cost Gas Supplies
• Utility Financial Crisis
• Substantial Load Growth
• Lack of New Generating and Transmission Capacity
• Aging Fleet of Power Plants
• Low Hydro Conditions
• Transmission/ Environmental Constraints
Electric Power
Supply/ Demand Imbalance
Power Disruption
Reduced Gas Supply
Power Disruption
First-Order Effects
Second-Order Effects
Third-Order Effects
Gas Supply
Curtailed Natural Gas Production
Oil Pipelines
Disruption of Product Pipelines
Water
Disruption of Irrigation Pumps
Cogen-eration
Reduced Steam Injection for Heavy Oil Production
Refineries
Inventory Buildup; Curtailed Operations
Storage Terminals
Inventory Drawdown; Shortages of Gasoline and Jet Fuel
Agriculture
Crop Losses
Oil Production
Reduced Heavy Oil Production
Road Transportation
Shortages of Specially Formulated Gasoline
Air Transportation
Disruption of Flight Schedules
Banking and Finance
Financial Losses

From Rinaldi et al.

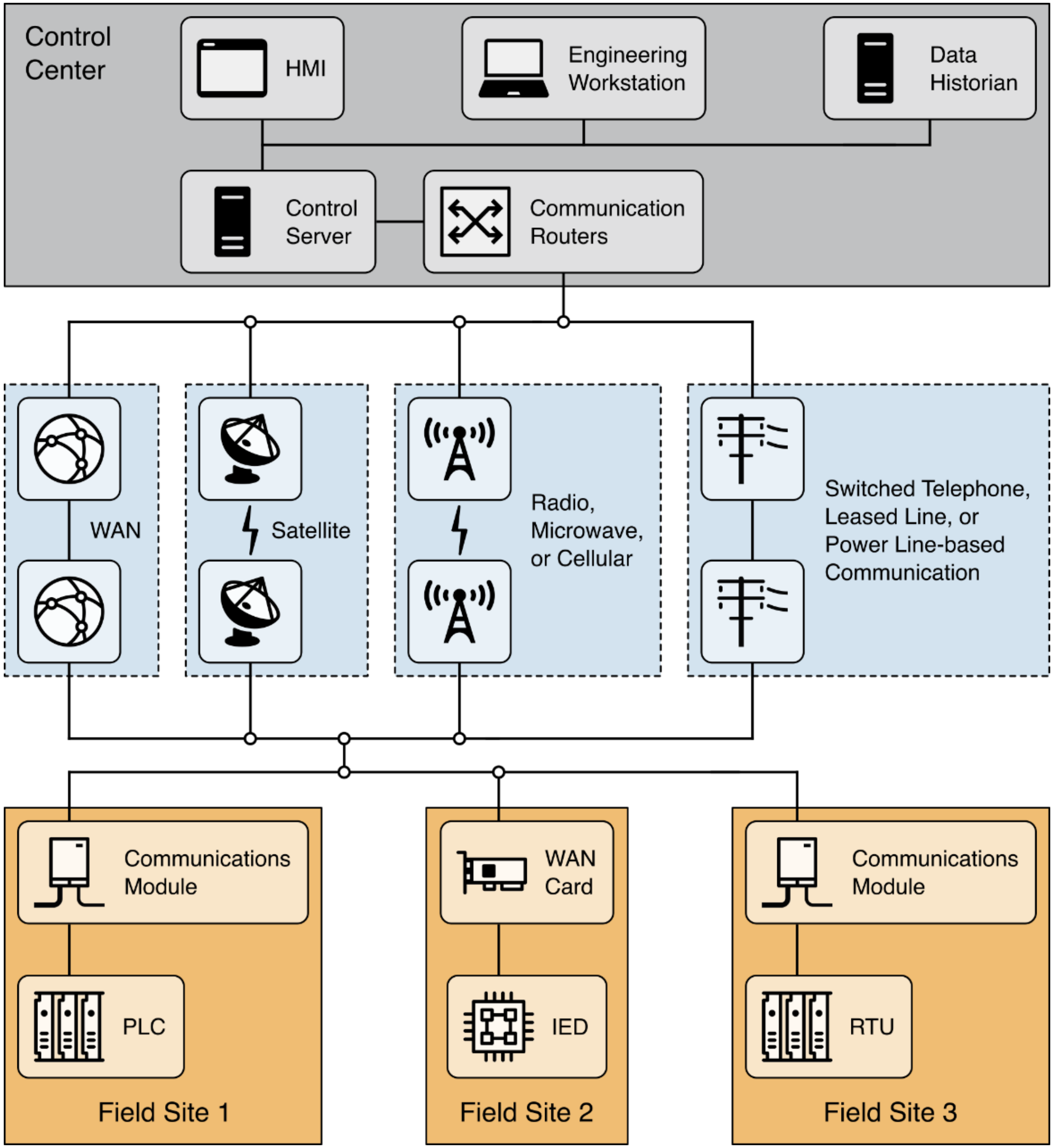
UK Power Outage, August 2019

- 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

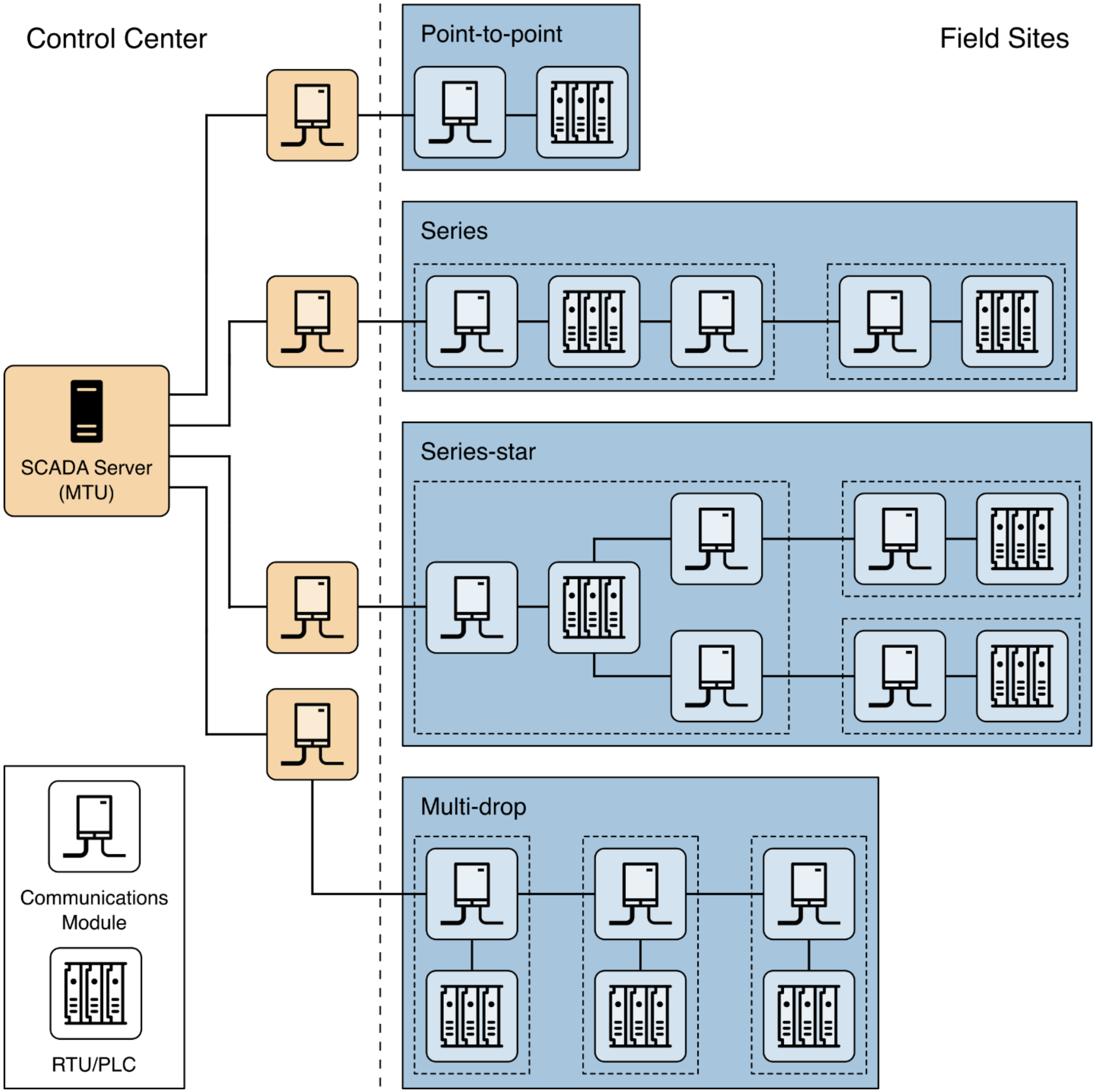
- Control Timing Requirements
- Geographic Distribution
- Hierarchy
- Control Complexity
- Availability
- Impact of Failures
- Safety

SCADA System Layout



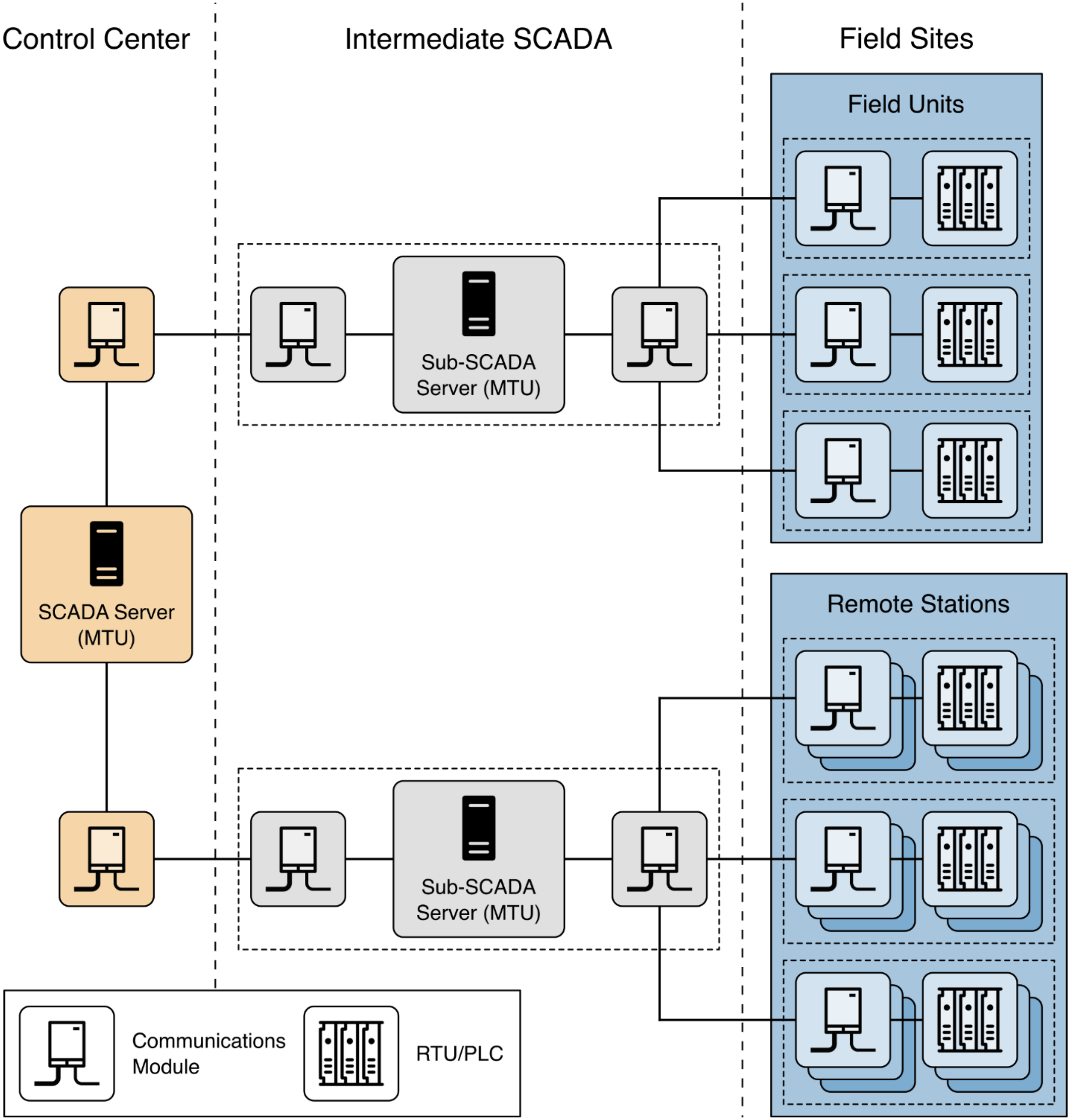
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Basic SCADA Comms Topologies



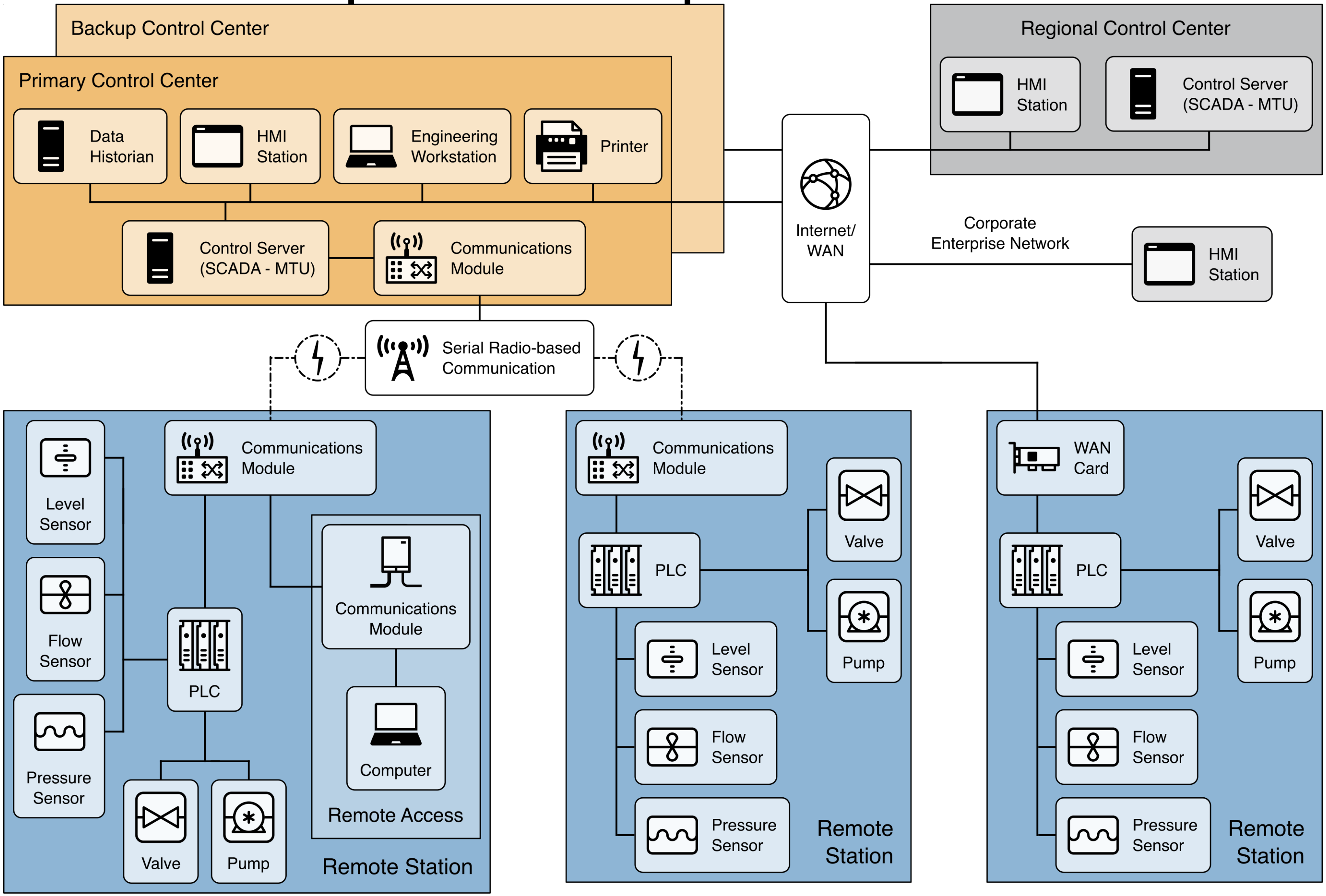
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Comms Topology For Larger SCADA Systems



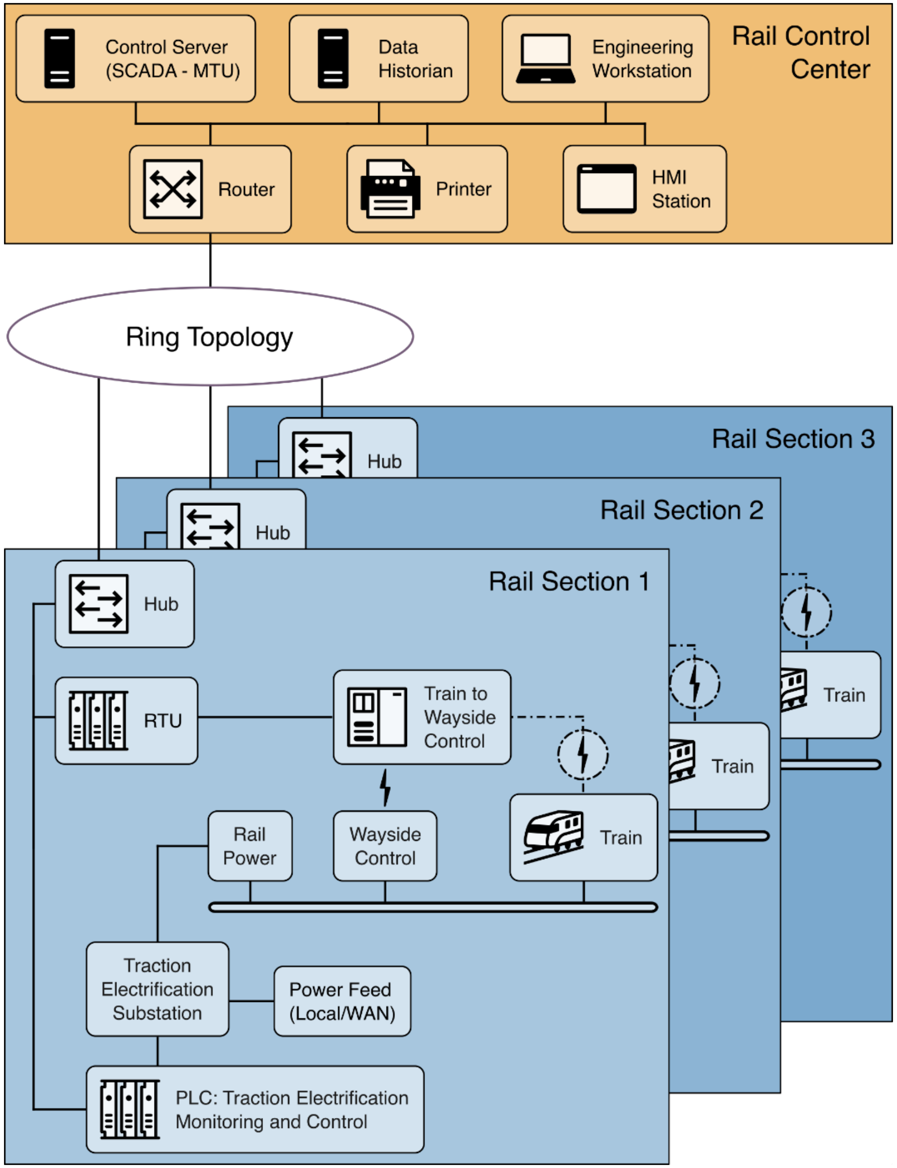
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Example of Implementation



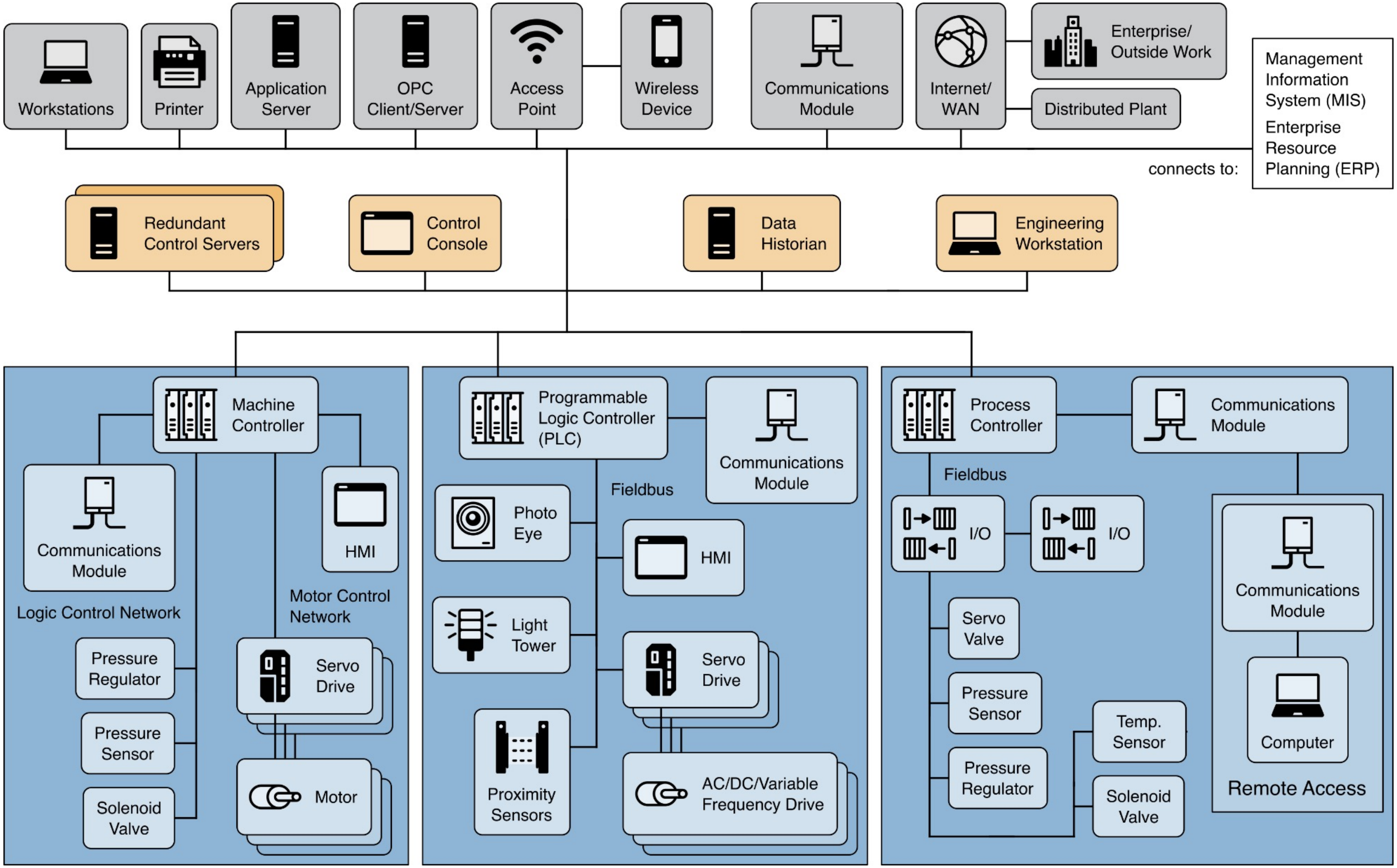
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Rail Monitoring and Control



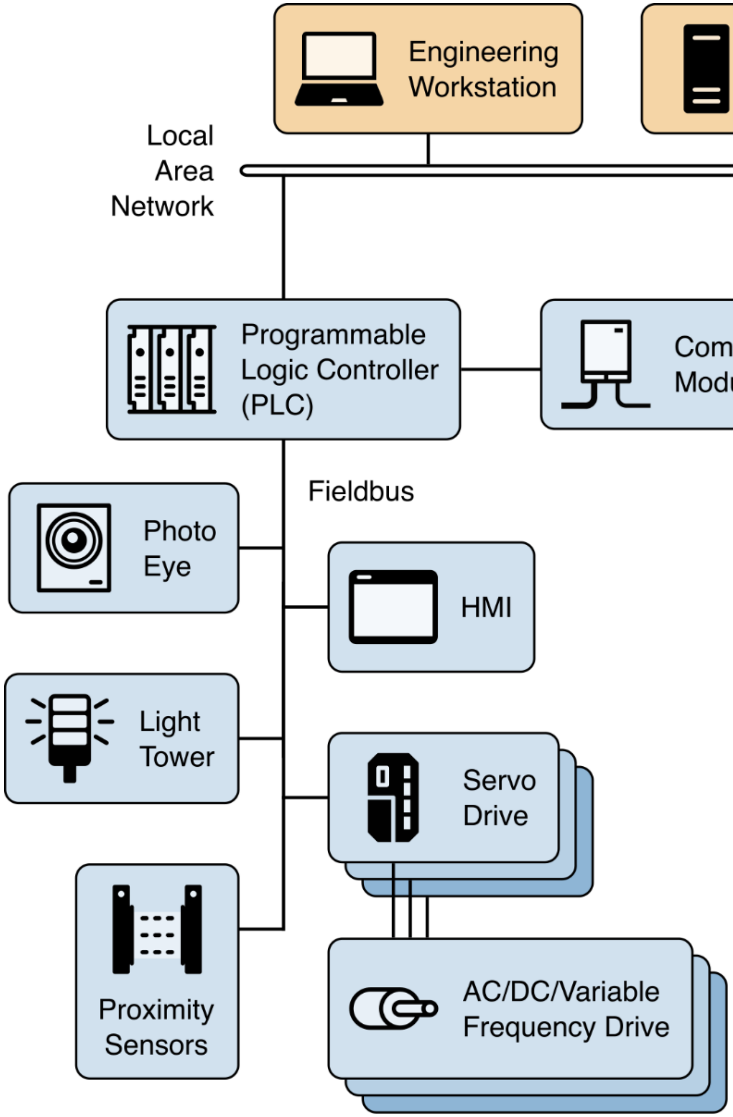
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

DCS Implementation



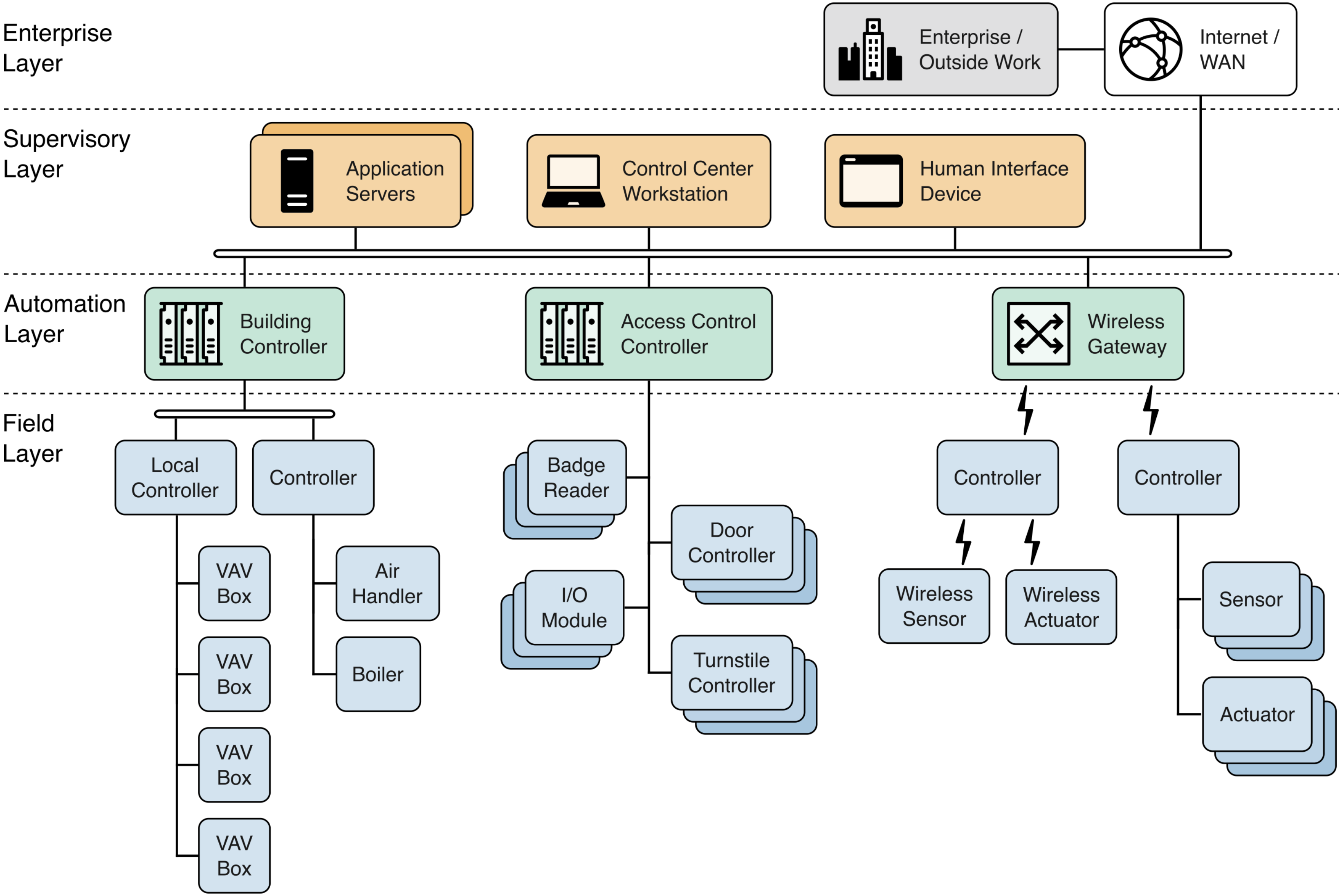
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

PLC Control System Example



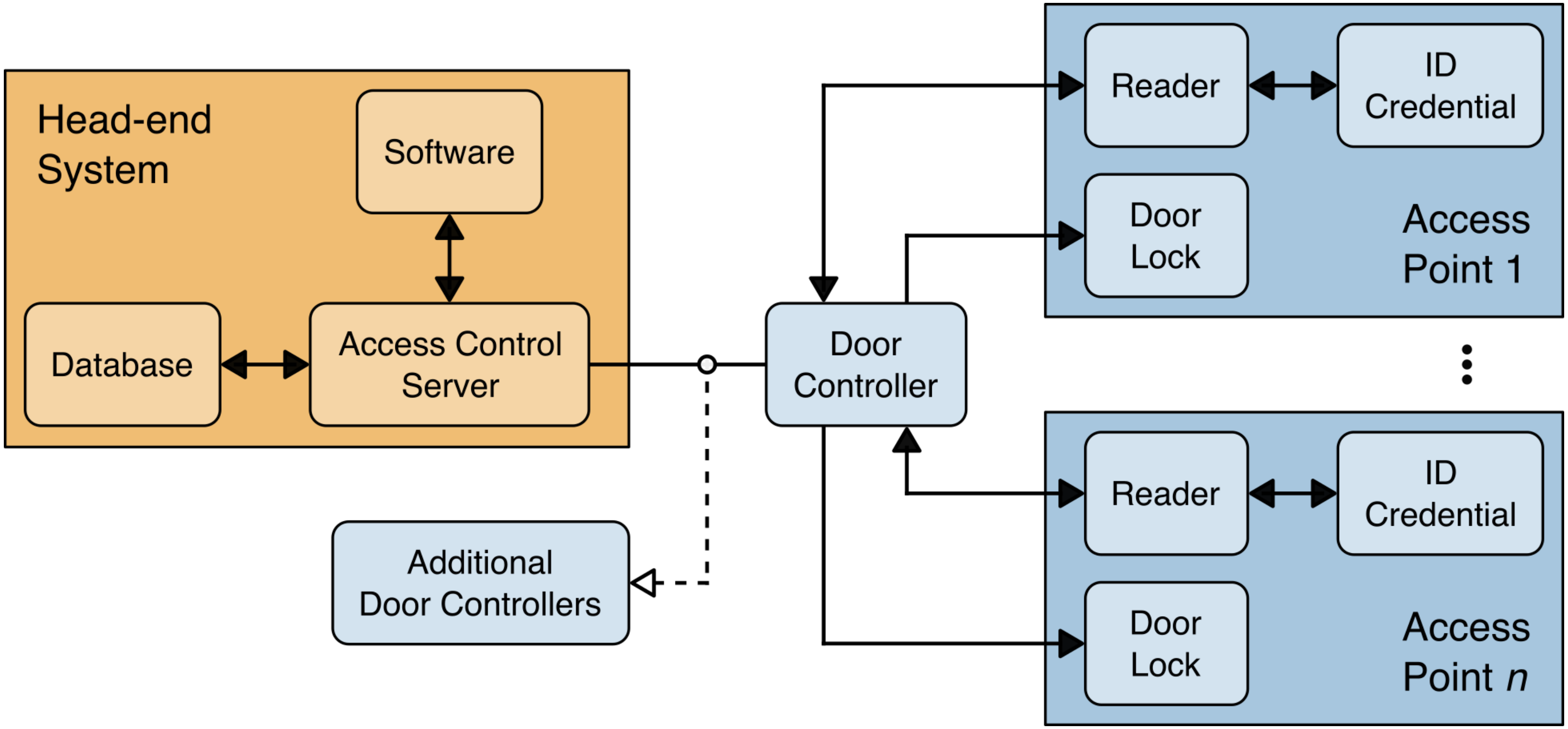
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Building Automation Systems



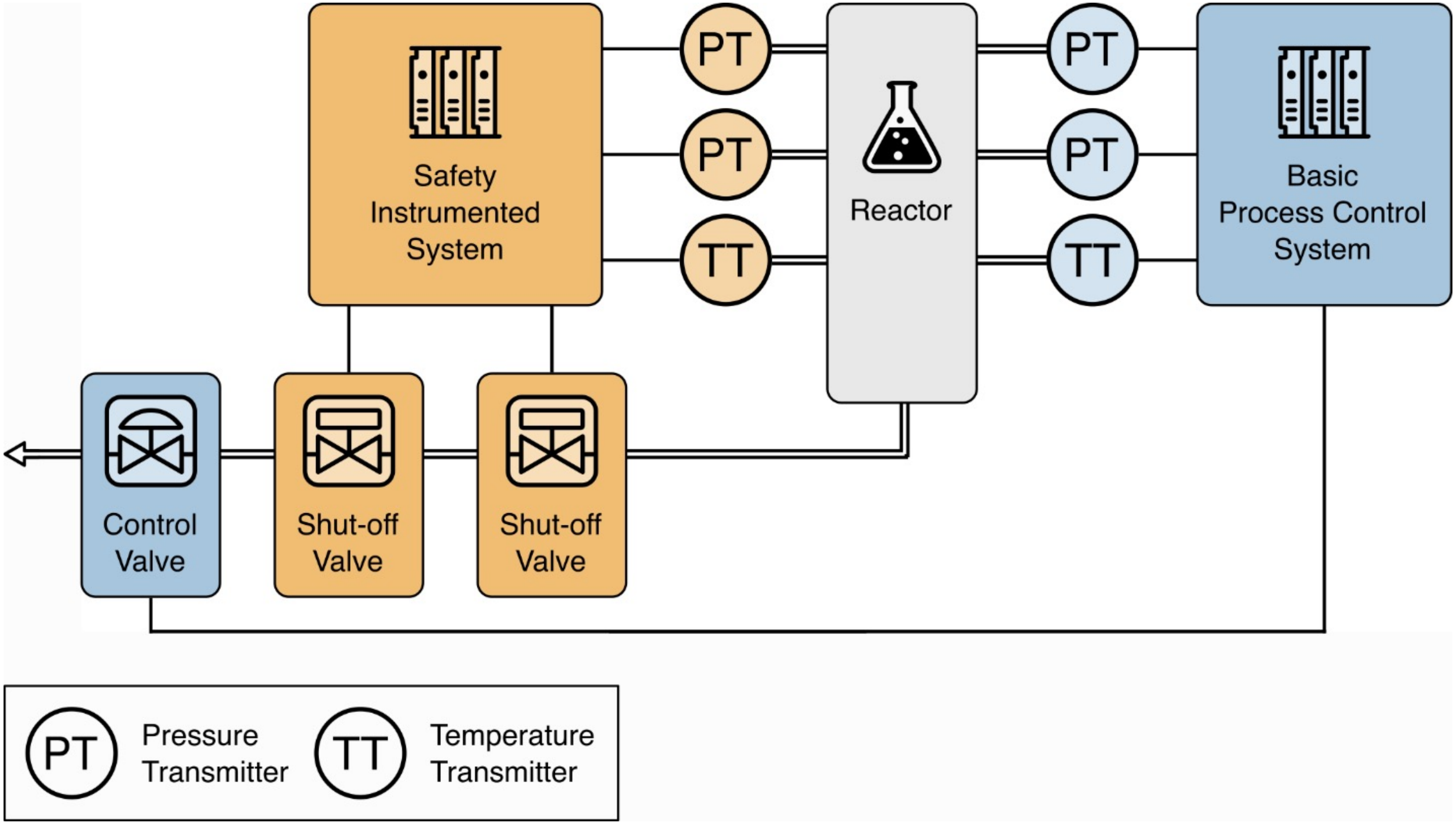
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Physical Access Control Systems



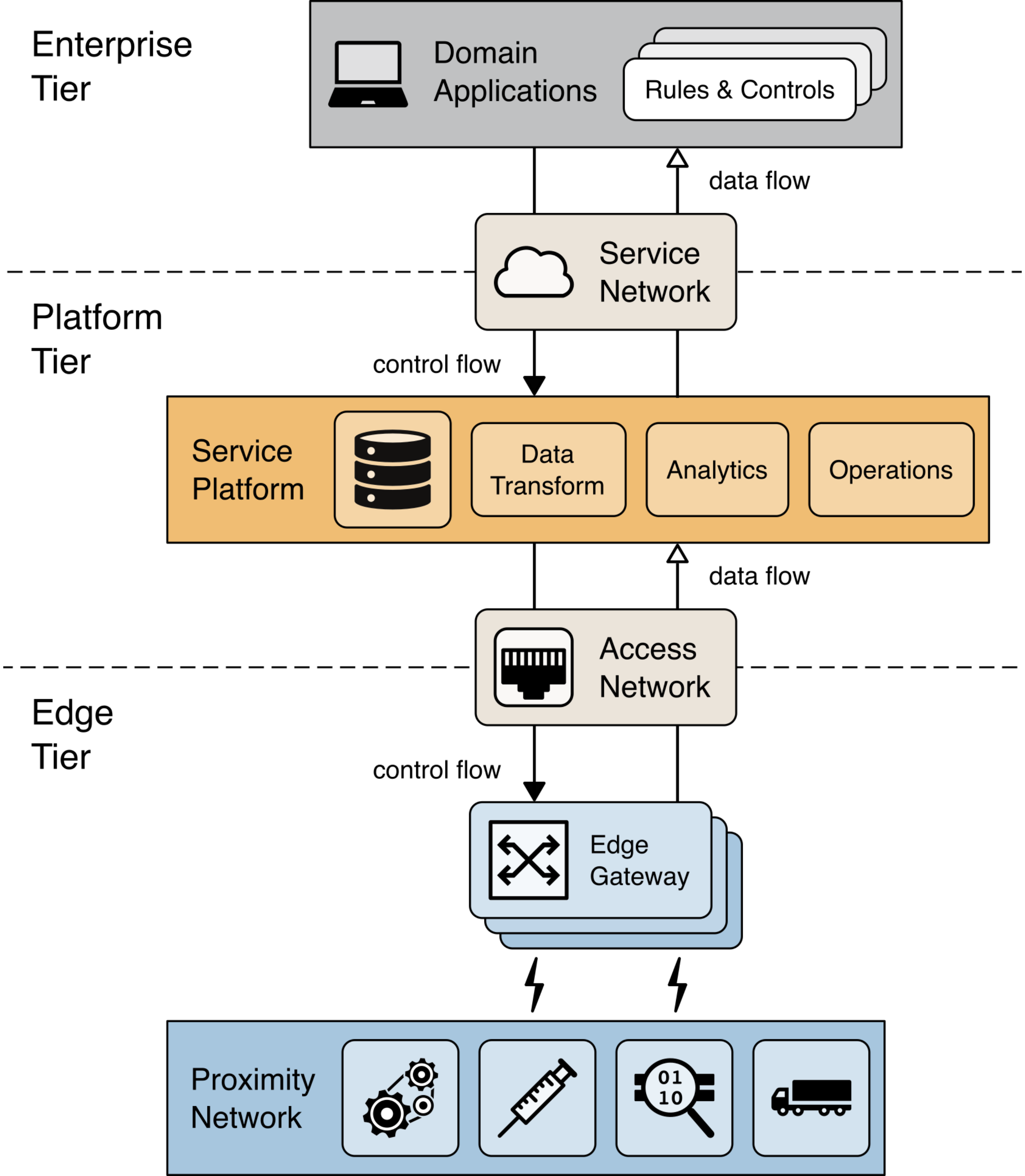
From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Safety Instrumented Systems



From NIST sp 800-82 (r3): Guide to Industrial Control Systems (ICS) Security

Industrial IoT



From NIST sp 800-82 (r3):
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)

Seven Strategies to Defend ICSs

Implement Application Whitelisting – 38%

Ensure Proper Configuration/Patch Management – 29%

Reduce your Attack Surface Area – 17%

Build a Defendable Environment – 9%

Manage Authentication – 4%

Monitor and Respond – 2%

Implement Secure Remote Access – 1%