



---


**KENNESAW STATE**  
UNIVERSITY

**Module 8:  
Emulating a Physical  
System – SCADA Security**

**Supervisory Control Data  
Acquisition (SCADA)**

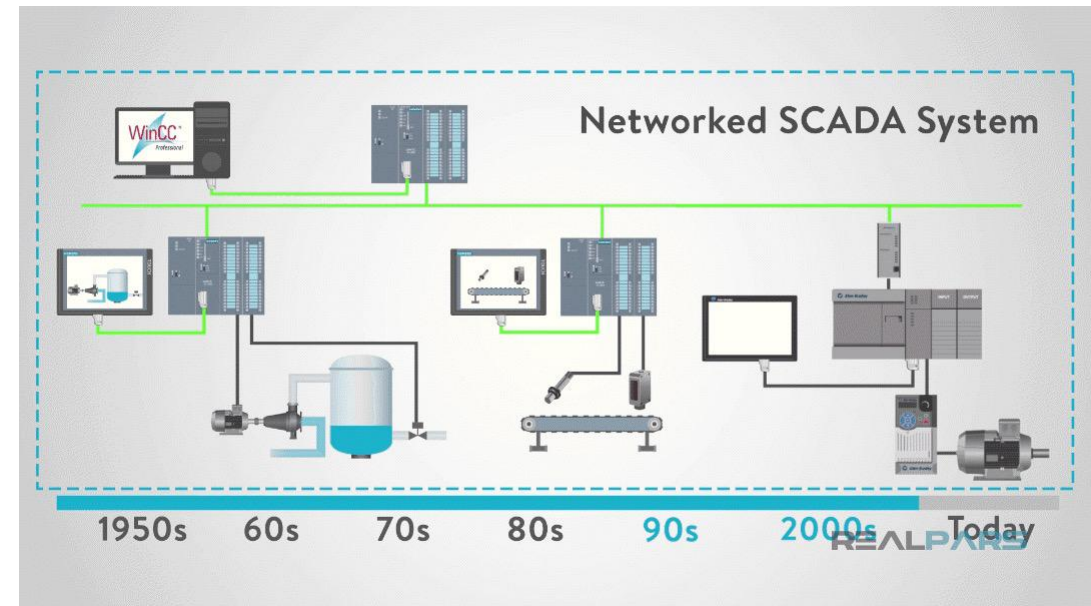
**Dr. Maria Valero**

# Agenda

- What is SCADA?
  - SCADA Components
  - How SCADA affects me?
  - Who would attack SCADA?
  - SCADA Security
  - Vulnerability Analysis in SCADA
- 

# What is SCADA?

- Real time industrial process control systems to monitor and control remote or local industrial equipment
- Vital components of most nation's critical infrastructures
- Risk of deliberate attacks!



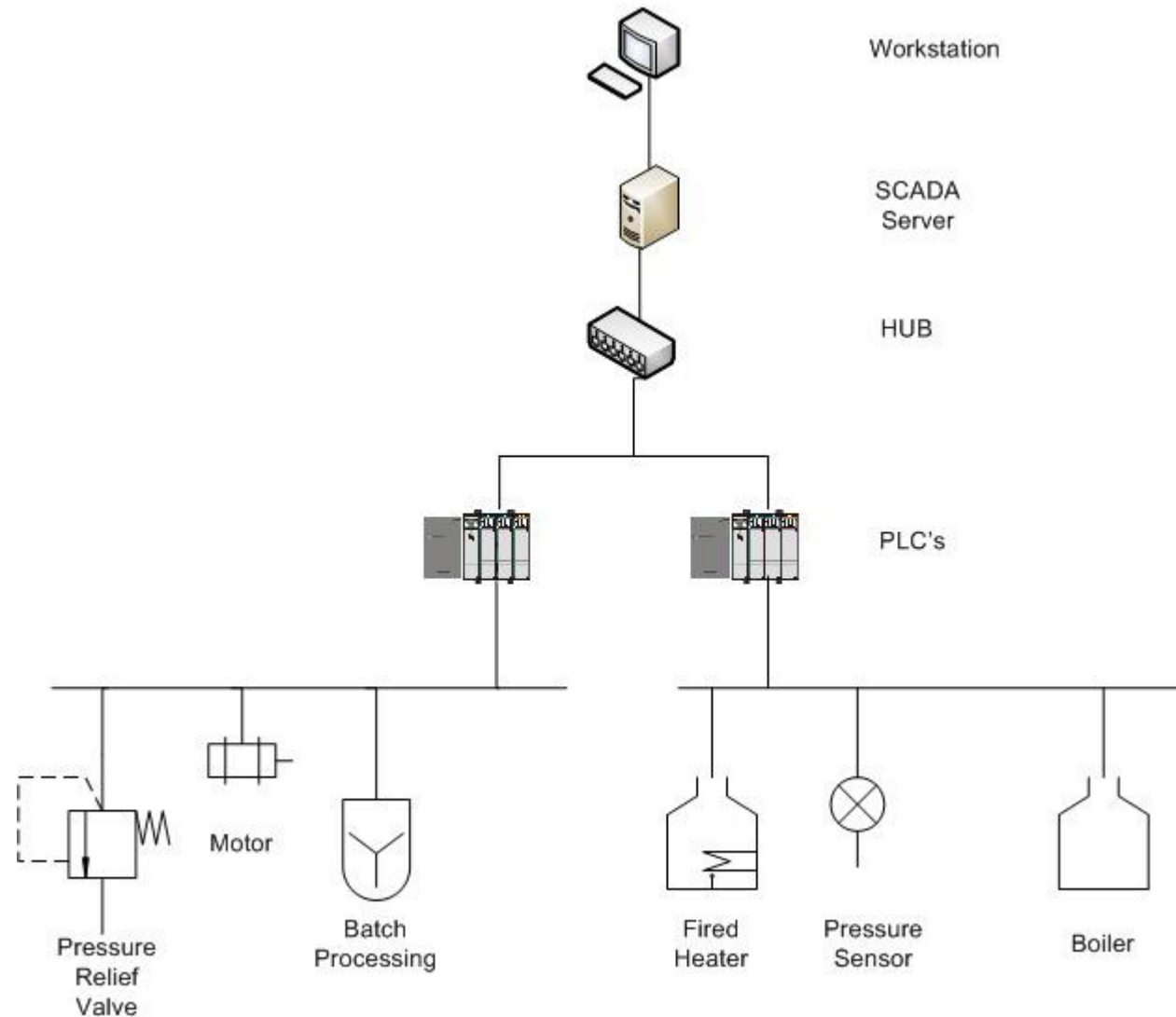
# SCADA Systems

- 1990: mainframe computer supervision
- 1970: general purpose operating systems
- 1990: off the shelf computing
- Highly distributed with central control
- Field devices control local operations

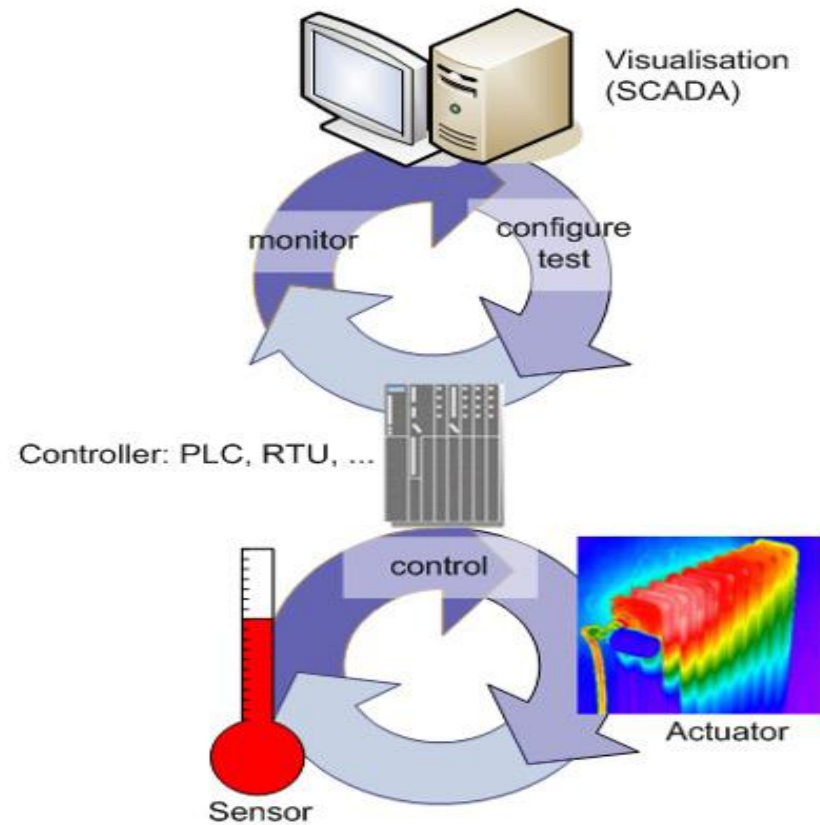
# SCADA Components

- **Corporate network segment**
  - Typical IT network
- **SCADA network segment**
  - Servers and workstations to interact with field devices
  - Human-machine interfaces
  - Operators
  - Software validation
- **Field devices segment**
  - Programmable Logic Controllers (PLC)
  - Remote Terminal Units (RTU)
  - Intelligent Electronic Devices (IED)

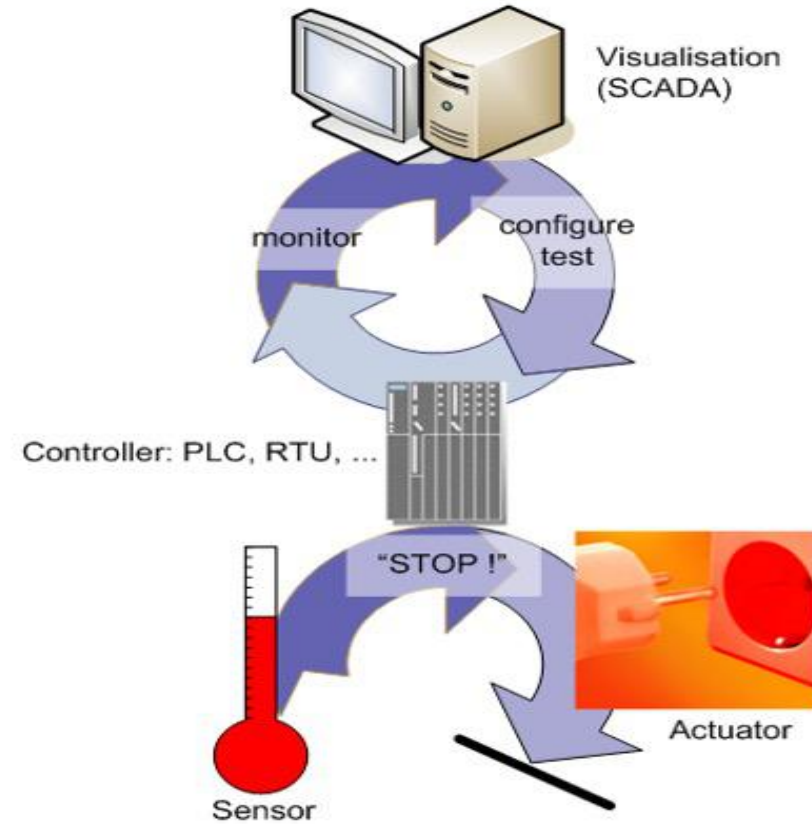
# SCADA and PLC Overview



# Process Control System (PCS)



# Safety System



# SCADA Incidents

- Flaws and mistakes
- 1986: Chernobyl Soviet Union
  - 56 direct death, 4000 related cancer death
- 1999: Whatcom Creeks Washington US pipeline rupture
  - Spilling 237,000 gallons of gasoline that ignited, 3 human life and all aquatic life
- 2003: North East Blackout of US and Canada
  - Affected 55 million people, 11 death
- 2011: Fukushima Daiichi nuclear disaster Japan
  - Loss of human lives, cancer, psychological distress



# How SCADA affects me?

- SCADA is a wide and generic term to indicate the whole of industrial control and monitoring systems that:
  - Provide power to your home
  - Bring water into your life
  - Control traffic lights onto the way to your office/school
  - Control the commuter train you are every day
  - Handle the air conditioning in your office
  - Allow you to call your wife to tell her you'll late
- I'd say it pretty much affects everyone of us, won't you?


Who would attack  
SCADA?

---

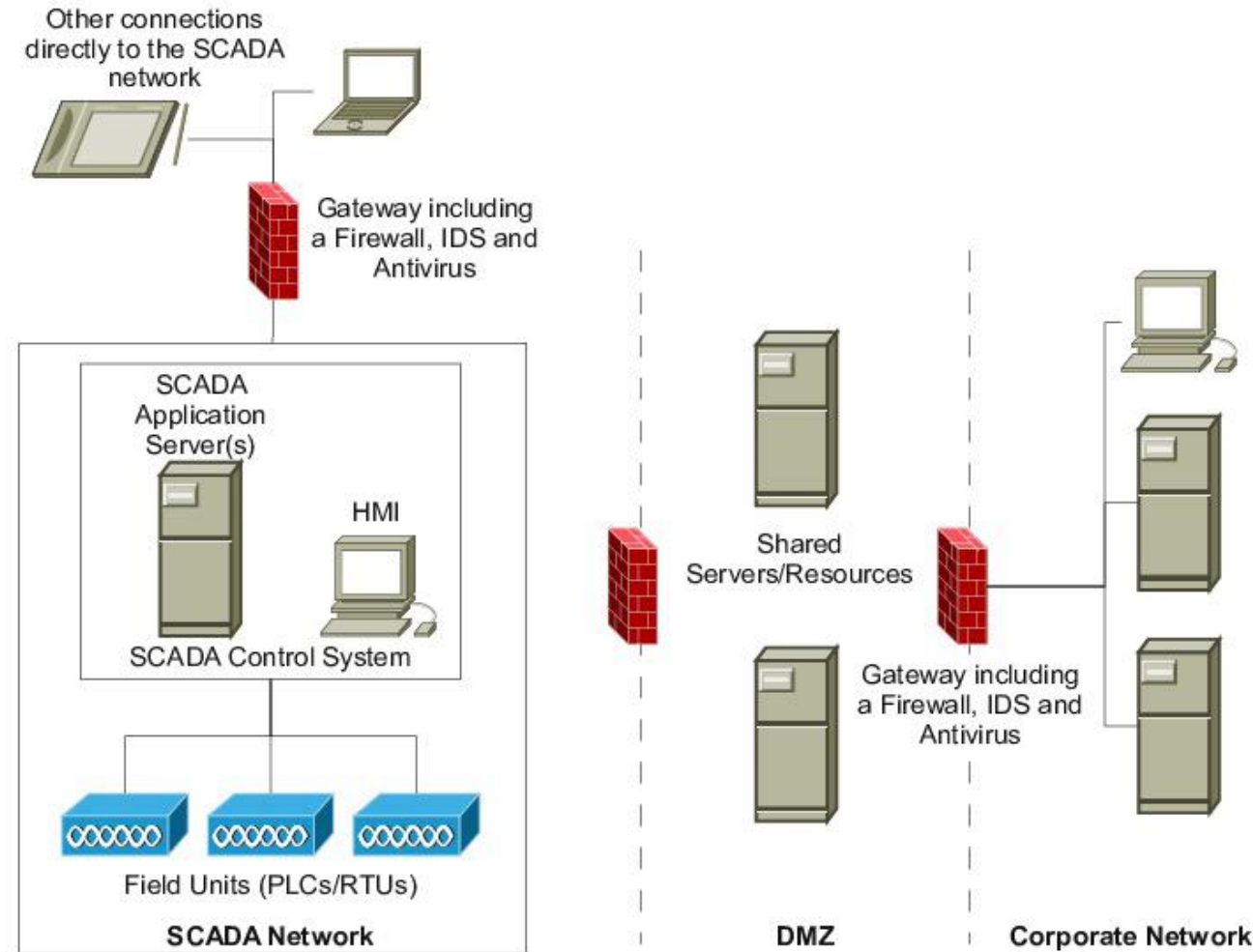
# Attackers

- Script kiddies
- Hackers
- Organized crime
- Disgruntled insiders
- Competitors
- Terrorists
- Hactivists
- Eco-terrorists
- Nation states

# SCADA Security (1)

- **Perimeter Protection**
    - Firewall, IPS, VPN, AV
    - Host IDS, Host AV
    - DMZ
  - **Interior Security**
    - Firewall, IDS, VPN, AV
    - Host IDS, Host AV
    - NAC
    - Scanning
  - **Monitoring**
  - **Management**
- 

# SCADA Security (2)



# Programmable Logic Controllers (PLC)

- Computer based solid state devices
- Control industrial equipment and processes
- Regulate process flow
  - Automobile assembly line
- Have physical effect

# Related Work (1)

- Security working groups for the various infrastructure sectors of water, electricity and natural gas
- US Departments of Energy and Homeland Security: investigation into the problem domain of SCADA systems

# Related Work (2)

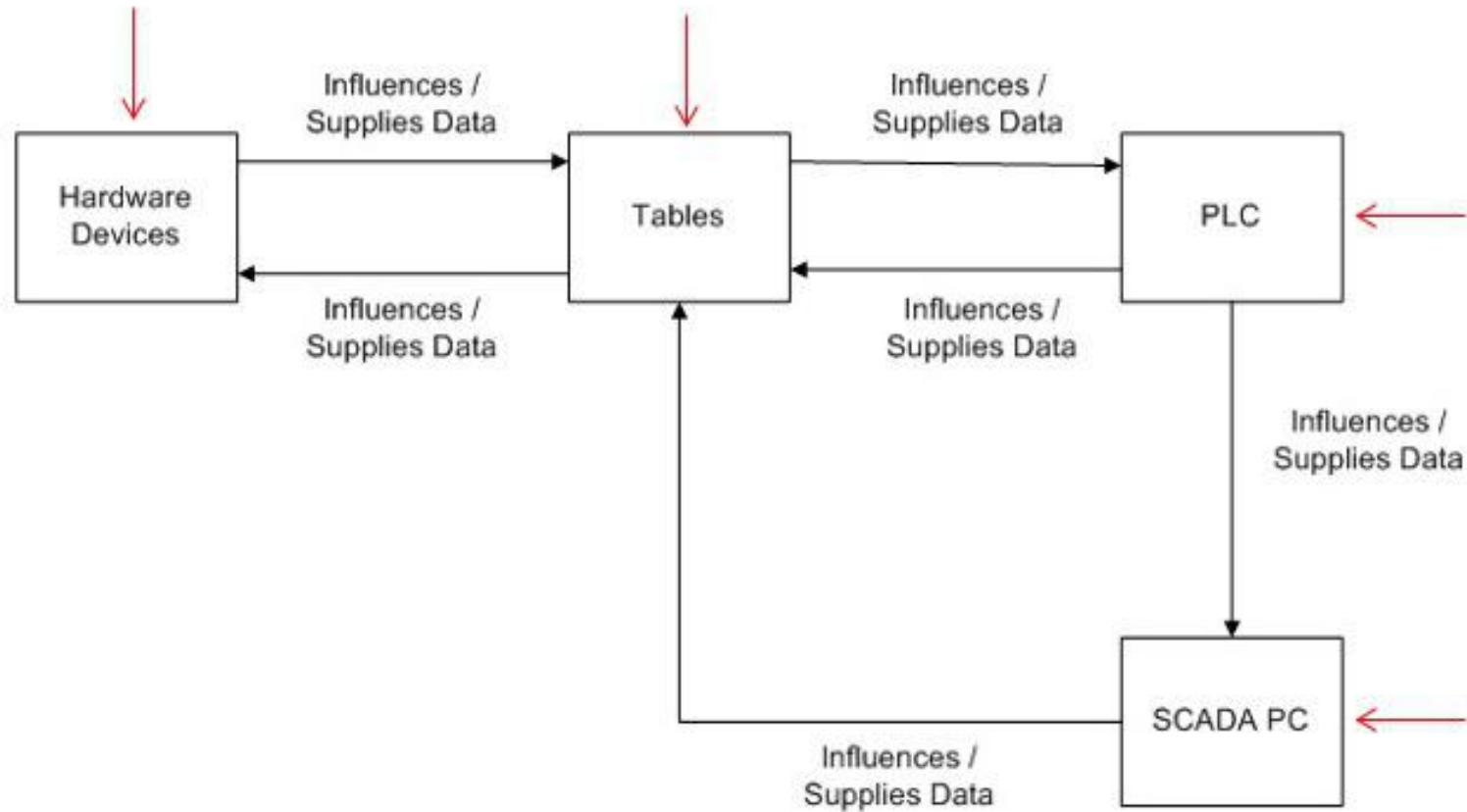
- Traditionally vendors focused on functionality and used physical security measures
- An attempt was made to try to “match” physical security mechanisms online
- Vulnerabilities:
  - Classification by affected technology
  - Classification by error or mistakes
  - Classification by enabled attack scenario



# SCADA and PLC Security (1)

- Increased risk to SCADA systems, introduces another element of risk to the PLC and all of the control elements
  - PLC's dictate the functionality of the process
  - PLC programming software and SCADA control software can be housed on the same machine
- The newest PLC hardware devices allow for direct access to the PLC through the network

# SCADA and PLC Security (2)



SCADA System Control Flow

# SCADA and PLC Security (3)

- Prior to the Stuxnet attack (2010): it was believed any cyber attack (targeted or not) would be detected by IT security technologies
- Need: standard be implemented that would allow both novice and experience PLC programmers to verify and validate their code against a set of rules.
- How do we show that PLC code and be verified and validated to assist in the mitigation of current and future security risks (errors)?

# Vulnerability Analysis in SCADA

1. Attack Severity Analysis
2. Building the Vulnerability Taxonomy
3. Potential Exploitation of Coding Errors

# 1. Attack Severity Analysis (1)

Severity	Effects in PLC	Effects in SCADA
A	PLC Code will not perform the desired tasks	Will not allow for remote operation of the process
B	Serious hindrance to the process	The process could experience intermittent process failure
C	Adversely effects PLC code performance. A minimal cost effect to the project, but a “quick fix” is possible	Data shown on the SCADA screen is most likely false
D	Effects the credibility of the system, but the PLC code is operable	Incorrect data could be randomly reported, cause a lack of confidence in the system

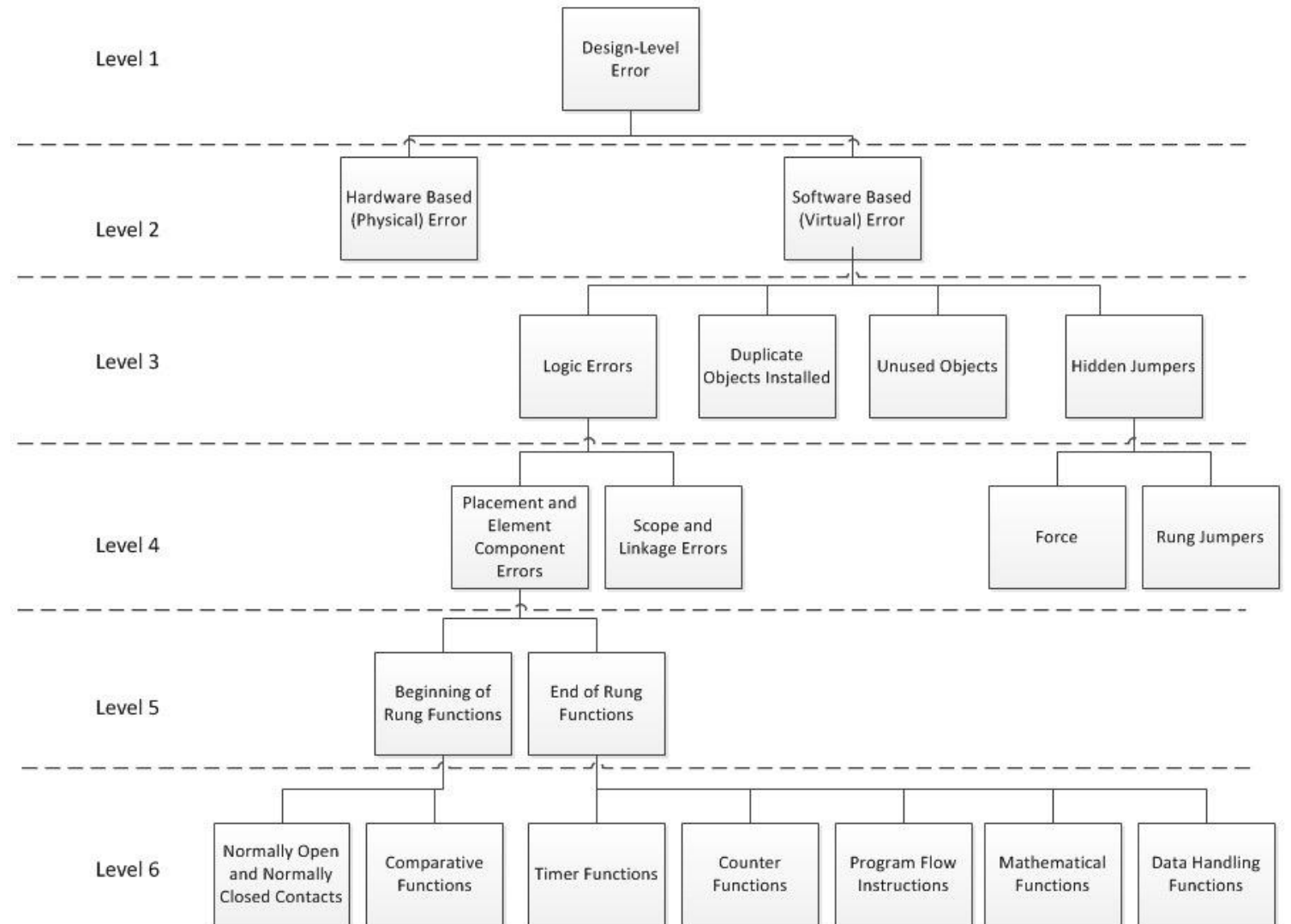
- Each row of the Severity Chart represents a different level of security risk, within the PLC error found
- The error levels range from A – D, with A being the most severe and D being the least severe
- Each column represents the effects which can occur in the PLC and those that can occur in the SCADA system PC

# 1. Attack Severity Analysis (2)

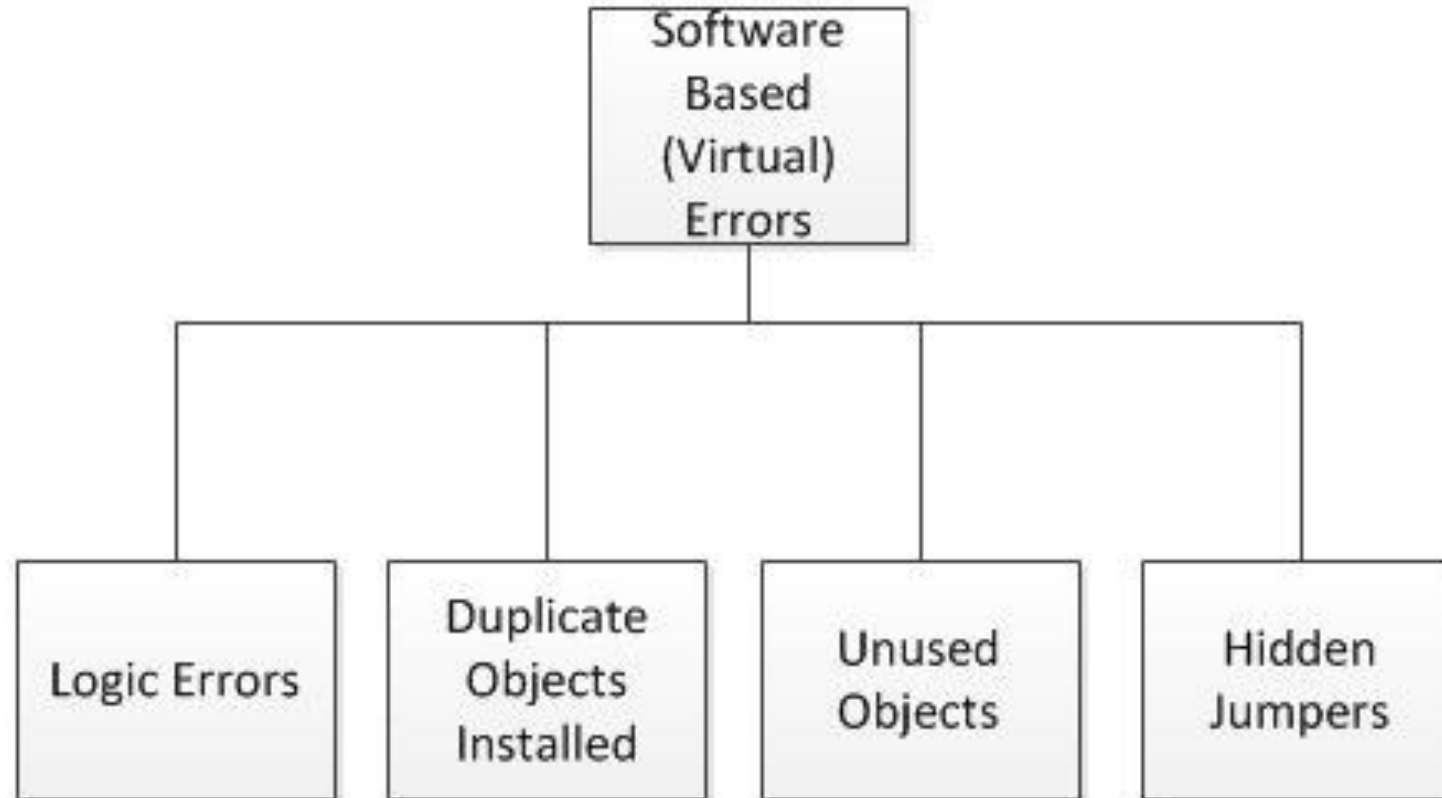
- Severity Classifications:
  - Severity Level A: Could potentially cause all, or part, of a critical process to become non-functional.
  - Severity Level B: Could potentially cause all, or part, of a critical process to perform erratically.
  - Severity Level C: Denote a “quick fixes”
  - Severity Level D: Provide false or misrepresented information to the SCADA terminal.

# 2. Building the Vulnerability Taxonomy (1)

- Purpose:
  - To aid the process of detecting these vulnerabilities in the PLC code
- Intended to be extensible
  - Created such that it can be expanded as:
    - Future versions of PLC's are created
    - New errors are found



## 2. Building the Vulnerability Taxonomy (2)



Vulnerability Taxonomy: Software Based (Virtual) Errors



# 3. Potential Exploitation of Coding Errors

Error Type	Taxonomy Classification	Malicious User Opportunity
Process Critical / Nuisance	Duplicate Objects Installed	Alterations of one or more of the duplicate objects
Process Critical	Unused Objects	Pre-loaded variables allow for an immediate entry point into the system
Process Critical	Scope and Linkage Errors	Installation of jump to subroutine command which would alter the intended file to file interaction
Process Critical	Logic Errors	Immediate entry point to logic level components such as timers, counters, and arithmetic operations
Process Critical / Nuisance	Hidden Jumpers	Would allow for a placement point for a system bypass