Improving Industrial Process Control Systems Security

Uwe Epting (TS/CSE)
Maria Carmen Morodo Testa (TS/CV)

Security Problems

- General: EVERY computer connected to a network is exposed to security risks!
- 2 types of threats
  - Accidental “attacks”
    - Human errors
    - Security scans
  - Malicious attacks
    - Aggression
      - Login/passwords stolen
      - Sabotage
      - Switching equipment on or off
    - Viruses and worms
      - Automatic propagation
      - Data damage or manipulation
      - Denial of service attacks

Hardware

- Servers
  - Mostly UNIX based (HP-UX, Solaris, Linux)
  - Very important for service, critical component
  - Less risk for attacks (today!)
- PCs
  - Windows or Linux
  - Widely used
  - Very high risk
  - Frequent updates and patches necessary
- PLCs and I/O cards
  - Very robust
  - Little protection possible (today)

Network

- Ethernet at CERN
  - General purpose network
    - Very hostile and exposed to outside world
    - Frequent attacks from outside
  - Technical network
    - Only accessible inside CERN
    - BUT: connected to General Purpose network (today)
  - “Private” networks
    - Profibus
    - Modbus

Guidelines

- CERN wide
  - Operational Circular No 5
    - accepted by every computer user at CERN
  - Security guidelines
    - http://cern.ch/security

    - CERN's Computer Security Recommendations
    - Password Recommendations at CERN
    - Risks and how you can help to reduce them

Control System Issues

- Awareness campaign
  - Risk
  - Impacts
  - Solutions
- Review critical systems
- Network segregation
  - Firewalls
  - Remote access through terminal servers
  - Monitoring
- Project engagement
  - Commitment from the beginning

Strategy

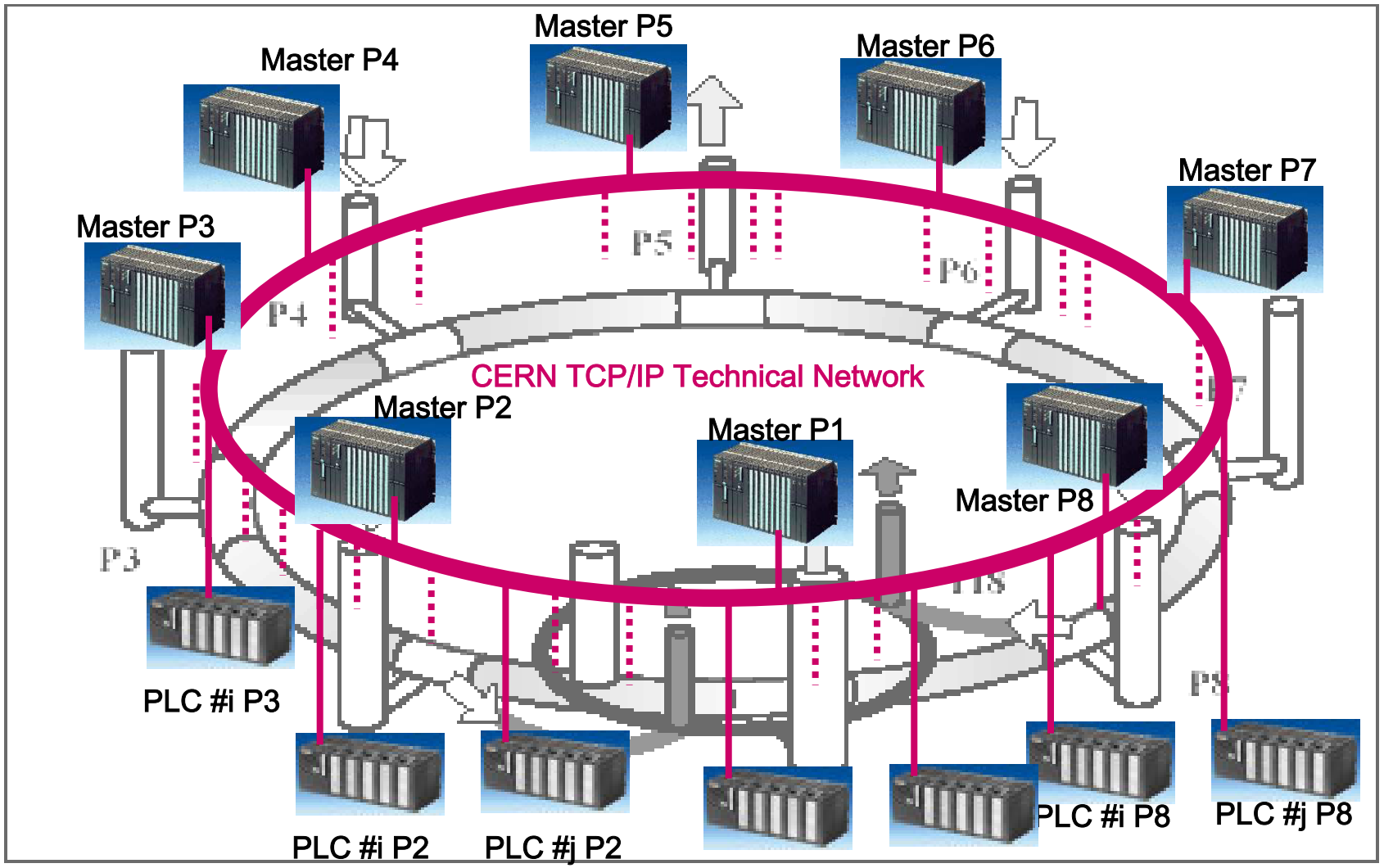
1. Understand the risk and engage projects early
2. Implement *Quick Win* security improvements
3. Manage third party risks
   - Vendors
   - Integrators
4. Establish security governance and response capability
5. Raise awareness and skills
6. Implement *Long Term* improvements
   - Network segregation, etc.

Example: LHC ventilation

1. Migration of LEP control system into LHC configuration
   - ~100 PLCs (+ ~50 micro-PLCs)
   - Motivations for upgrade:
     - Migration of the process control to the LHC functionality
     - Integration of systems
     - Replacement of obsolescent hardware and software
     - Recover and document the system know-how
2. Integration of control equipment for new LHC structures
   - ~25 new PLCs (+ ~125 new micro-PLCs)
3. Inter-point communication and CCC remote monitoring
   - 8 new master PLCs + 8 new SCADA platforms

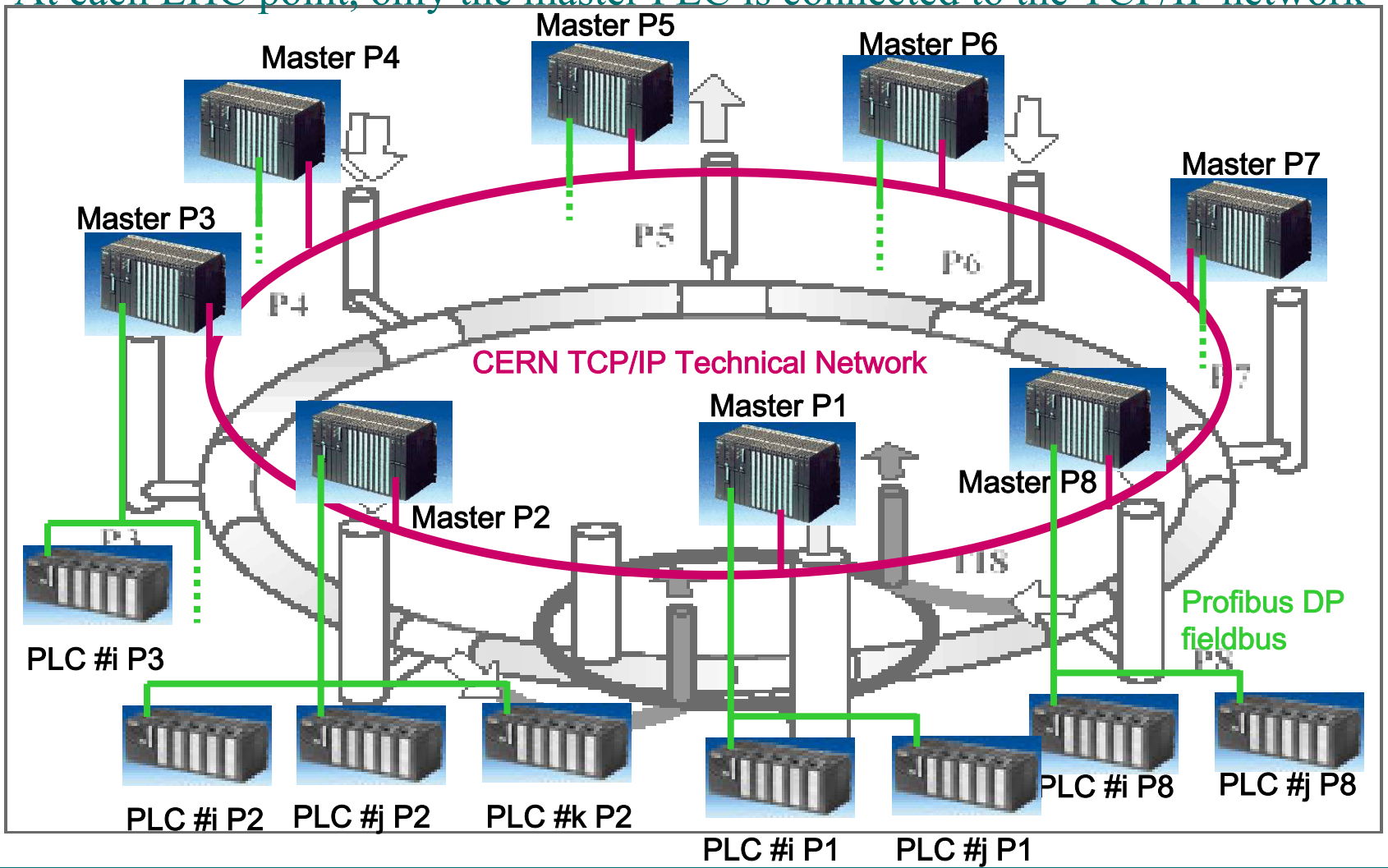
Technical Option #1

Every PLC is connected to the CERN TCP/IP network



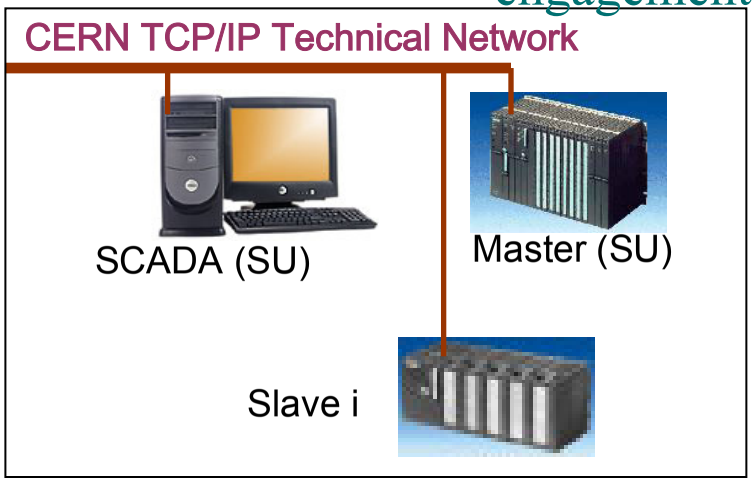
Technical Option #2

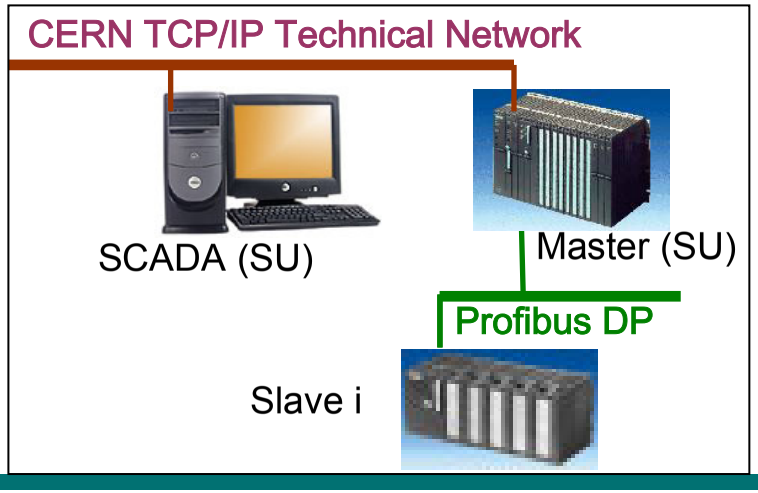
Every PLC is connected to a dedicated industrial fieldbus
At each LHC point, only the master PLC is connected to the TCP/IP network



Technical Options

Understand the risk: vulnerability increases with number of network connections ➡
***Quick win* improvement:** Profibus DP allows a compromise between openness and engagement to secure process control





Requirement / constraint	DP	TCP	Need (♠)
Availability	Very Good	Very Good	ESS
Security	Good	Needs plan	ESS
Remote accessibility (to slave PLCs)	Good	Very Good	DES
Project scheduling (time constraint)	Good	Good	ESS
Cost efficiency	Good	Good	ESS

(♠) ESS, *Essential;* DES, *Desirable*

Operational Aspects

Access to process control PLCs is now restricted ➡
Provisions are made to avoid limitations on the operational features

Local operation	1. An operation panel at each process control cubicle
	2. A supervision application at each LHC point (SUi)
	3. Local operation is possible from a laptop computer connected to the Profibus DP network (only intended for maintenance)
Remote operation	1. TIM interfaces with the master PLC at each LHC point
	2. Transmission of some relevant alarms and data from each LHC point by the means of a 2nd. path (MMD)
	3. Supervision application (SCADA) mimic diagrams web-published for remote information of operation teams

Conclusion

- Security issues are becoming a serious problem also at CERN
- "*Quick Win*" solutions do not require major investments if considered already in the design phase
- *"Long-Term"* solutions require clear CERN wide guidelines and regulations for the implementation of control systems
- Strategy to keep the systems up-to-date must be settled from the beginning. Continuous follow-up is needed to ensure secure O&M within the available and often limited resources

Questions ?