11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Securing SCADA critical network against internal and external threats

Anas ABOU EL KALAM[a], Mounia EL ANBAL[a,b], Siham BENHADDOU[b], Hicham MEDROMI[b] and Fouad MOUTAOUAKKIL[b]

[a] *IPI Paris, IGS Group, Paris, France*

[b] *Systems architectures Team, Hassan II University, ENSEM Casablanca, Morocco*

Plan

Problematic

Related work

Our vision

Advantages & Perspectives

General problematic

CRITIS 2016

Why are these networks targeted by hackers?

SCADA networks are least protected networks

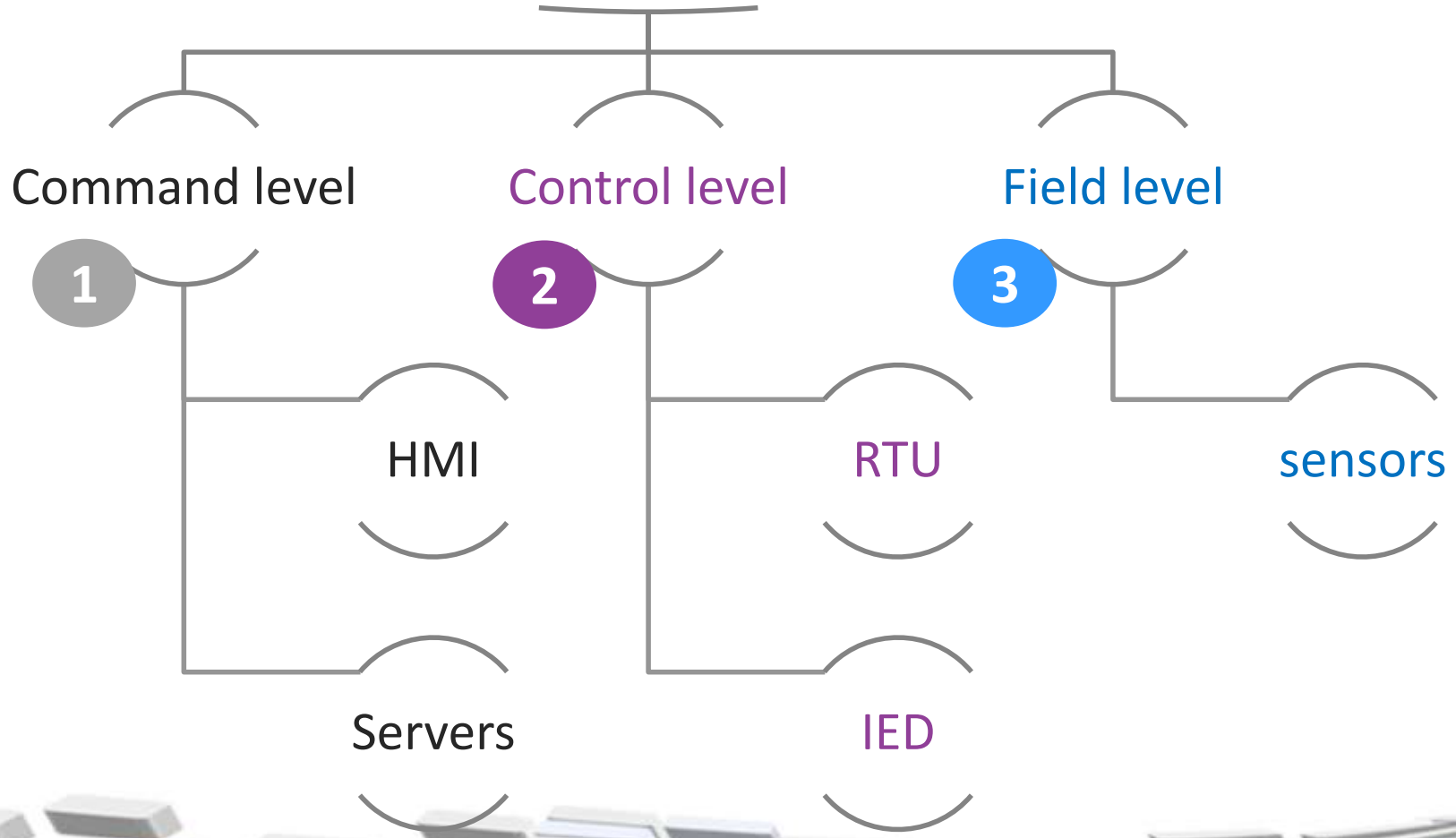
designed to operate 30 years but their openness to other IP networks had not been considered.

physical security has supplanted logical security on these networks [1]

Many new ICS and SCADA systems are open to Internet which allows the access and the use of ICS and SCADA infrastructure. This raised a number of new potential threats and vulnerabilities such as malware infection, DoS attacks, ...etc.

Related work

The SCADA architecture is a cluster architecture, it includes 3 levels:



Related Work

Approaches [8] et [5]

Approach [6]

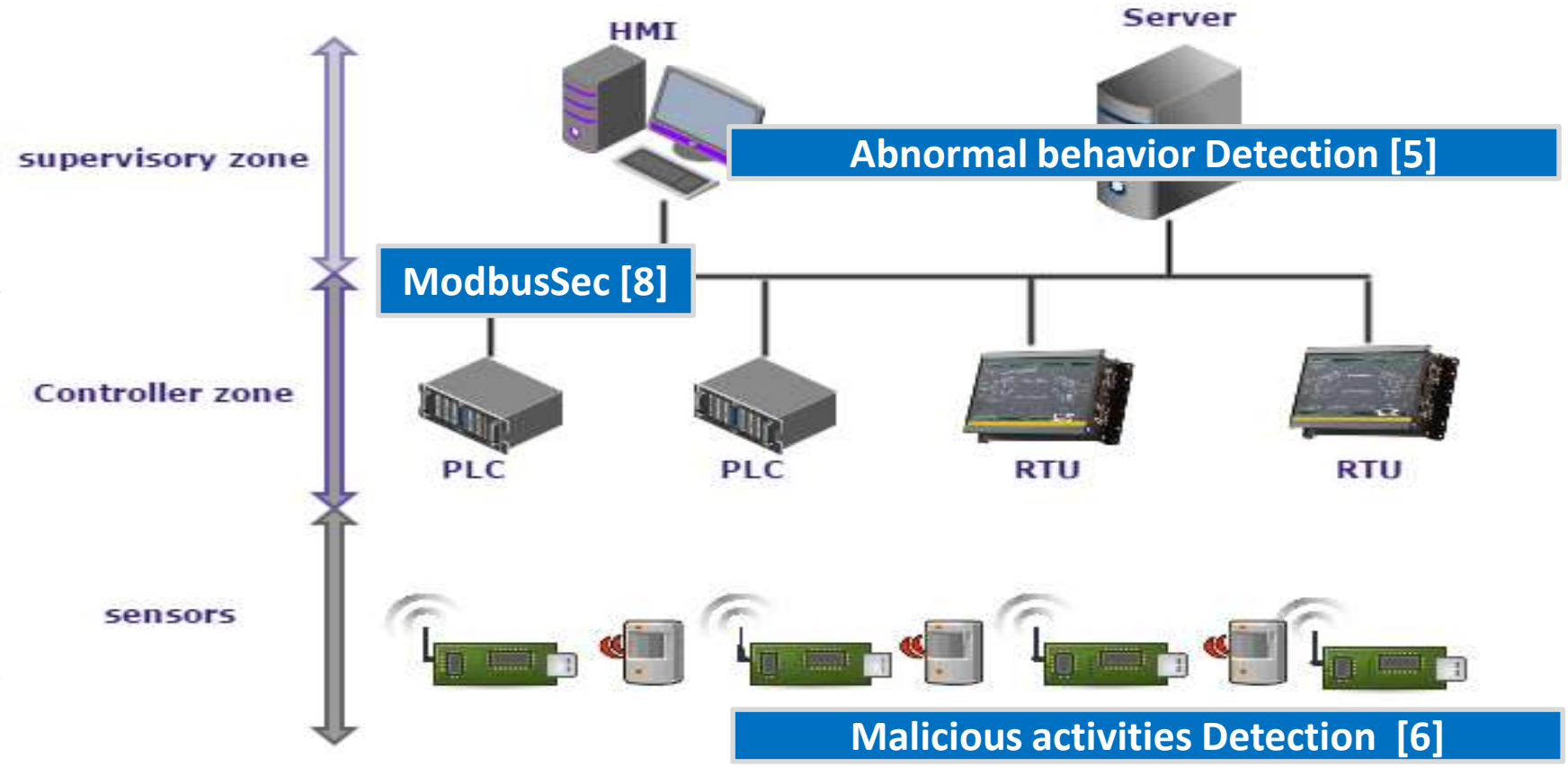


Figure 1: Example of a SCADA network environment

Approach 1 : Log monitoring strategy [5]

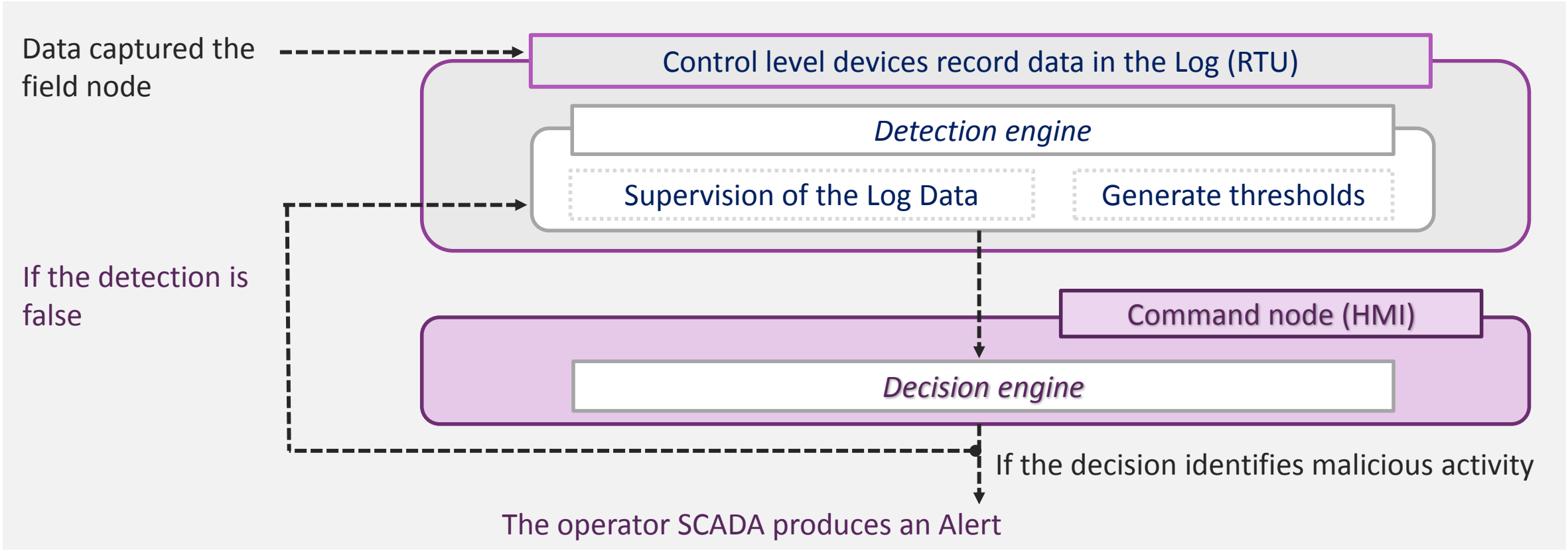
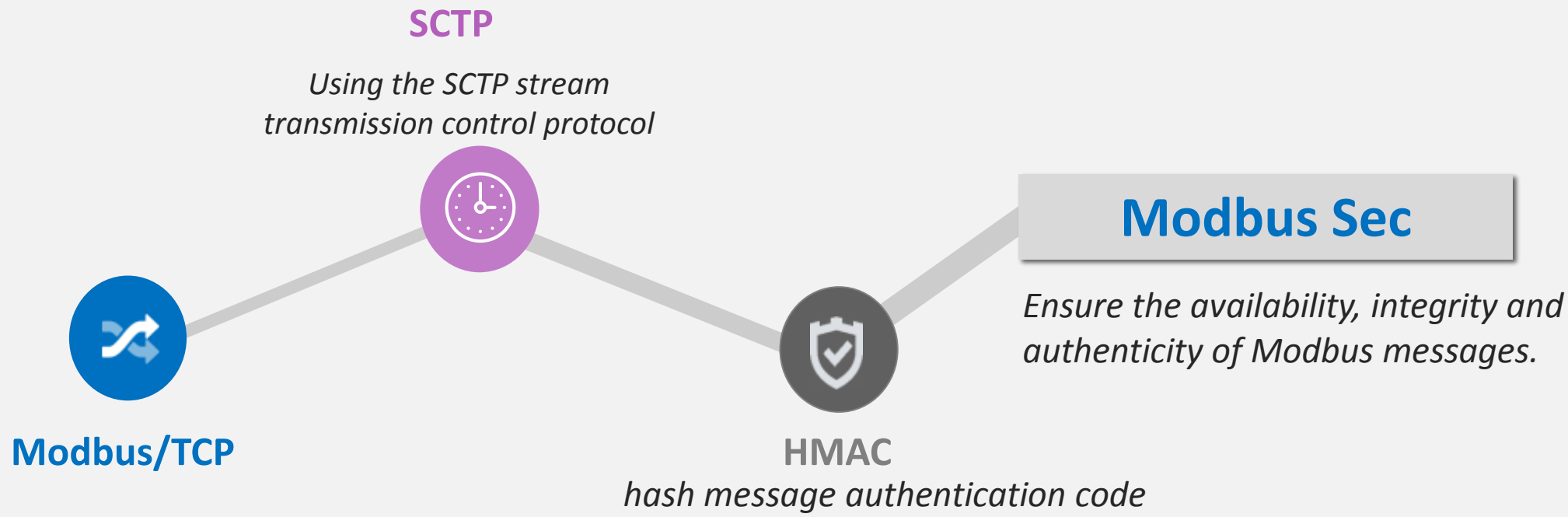


Figure 2 : Log monitoring architecture in SCADA System

Approach 2 : Secure Modbus using SCTP and HMAC [8]

- No Modbus feasible secure implementation exists.
- Modbus dependence on TCP as a transport mechanism has many inherent security risks
  - Increased susceptibility to denial of service attacks



Approach 3 : Modbus/TCP Packet monitoring [5]

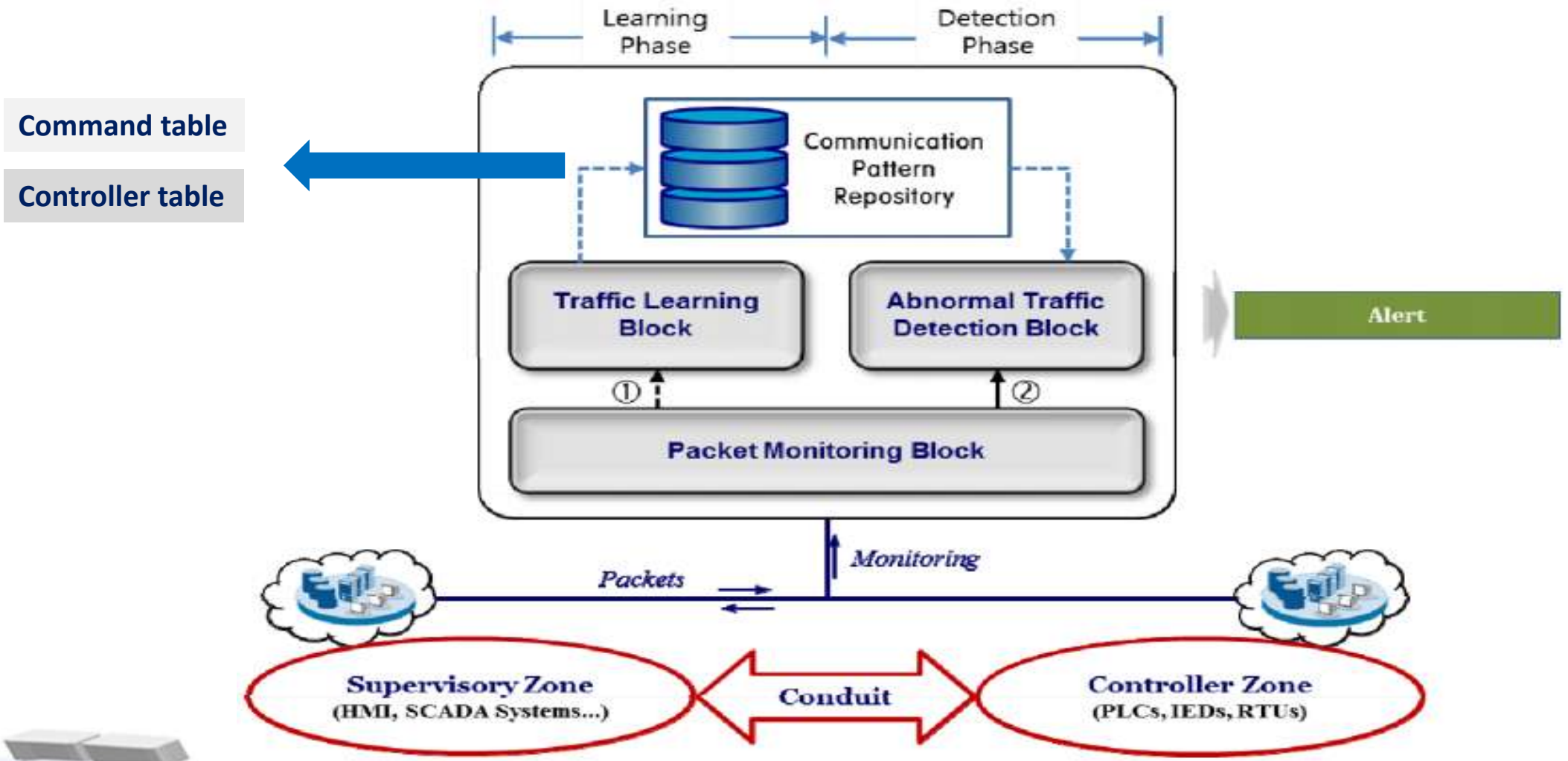
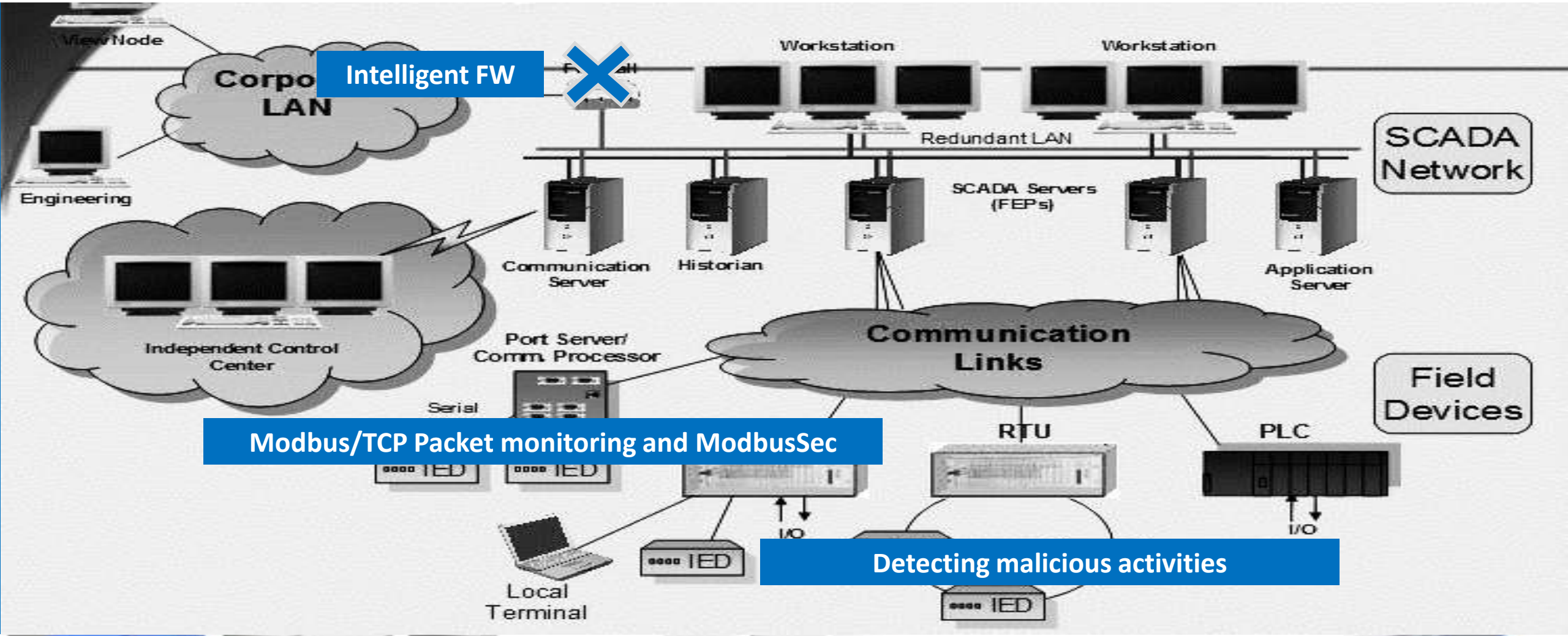


Figure 5 : Modbus/TCP packet monitoring

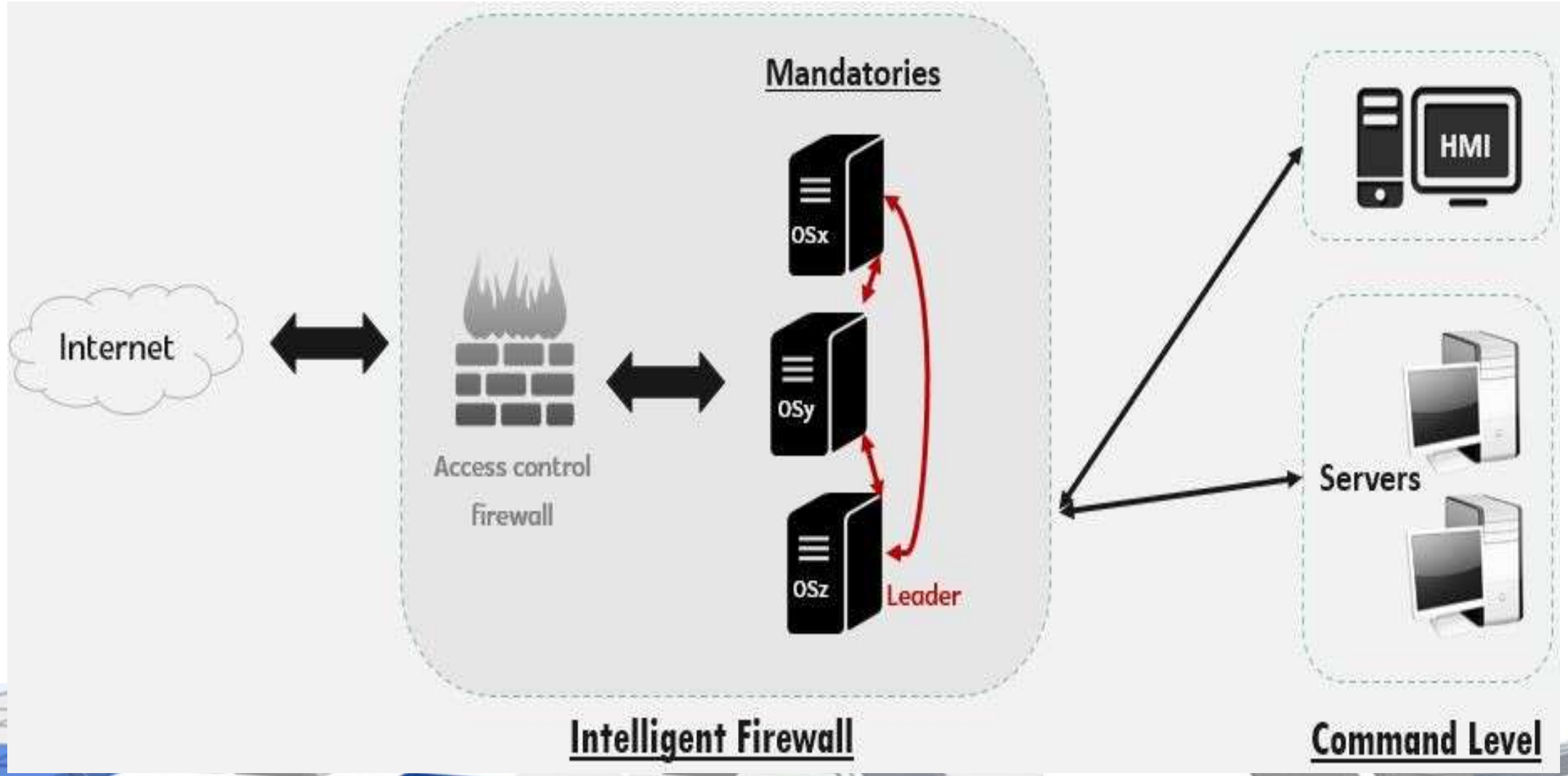
Analysis

1. No protection against Internal threats
2. No protection against External threats
3. No multi level protection
4. No recovery measure

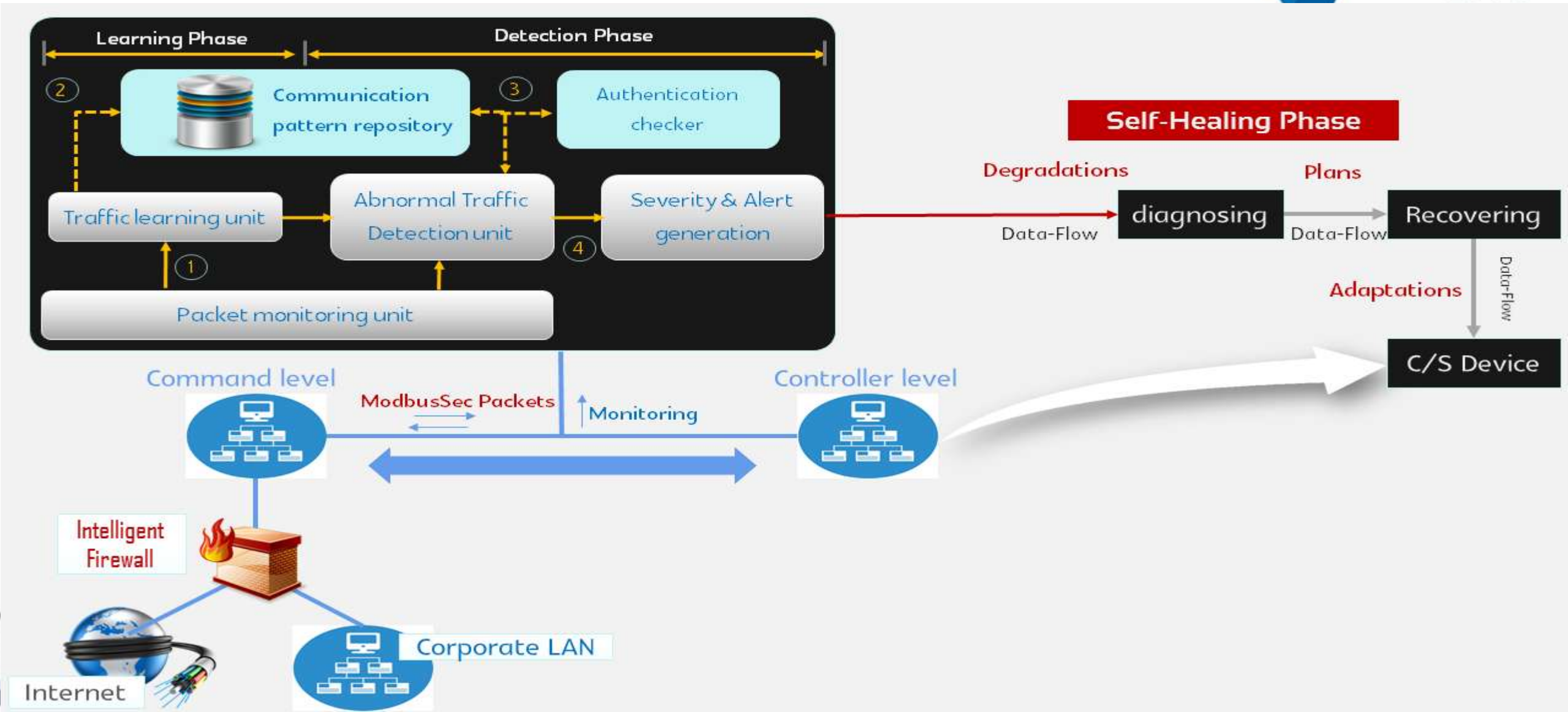
Our Vision


Intelligent FW
Workstation
Workstation
Redundant LAN
SCADA Network
Engineering
SCADA Servers (FEPs)
Communication Server
Historian
Application Server
Independent Control Center
Port Server/ Comm. Processor
Communication Links
Field Devices
Serial
Modbus/TCP Packet monitoring and ModbusSec
RTU
PLC
I/O
I/O
IED
IED
IED
IED
Local Terminal
Detecting malicious activities

The proposed Intelligent firewall



The proposed Architecture



Advantages & Perspectives

CRITIS 2016

Defense in depth

- Multi Layers protection

Self-Healing

- Recovery

Intrusion Tolerance

- Masking technique

Secure Communication Protocol

- Modbus Sec

Attack	Caused by	Solution	Zone
Any attacks	Internet	Intelligent firewall	Internet and command level
Message spoofing	Lack Device authentication	ModbusSec : HMAC	Command and control level
Replay attacks			
Denial of service			
Man-in-the-middle			
Doorknob-rattling attack	Access control	The occurrence of at least six failed logins in the log within 30 seconds	
Selective Forwarding and Black Hole attack	Compromised nodes	The mechanism uses acknowledgement (ACK)	Control and field level
Sybil attack	Malicious sensors	Our Log records the location with their Ids when a node sends data to its destination. If two identities are recorded from the same Location, Log infers that it is a malicious node.	
Jamming attack	Jammer nodes	If the traffic from the same Node Identity repeats for above or equal to a threshold value it may be from adversaries to cause jamming in the network	

Bibliography

1. Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, & Philip Chen, C. L. (2014). SCADA communication and security issues. Security and Communication Networks, 7(1), 175-194.
2. Psaier, H., Dustdar, and S.: A survey on self-healing systems: approaches and systems. Computing 91(1), 43–73 (2011)
3. Shahzad, A., Musa, S., Aborujilah, A., & Irfan, M. (2013, December). Se-cure Cryptography Testbed Implementation for SCADA Protocols Security. In Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on (pp. 315-320). IEEE.
4. Shahzad, A., Xiong, N., Irfan, M., Lee, M., Hussain, S., & Khaltar, B. (2015, July). A SCADA intermediate simulation platform to enhance the system security. In Advanced Communication Technology (ICACT), 2015 17th Inter-national Conference on (pp. 368-373). IEEE.
5. Kim, B. K., Kang, D. H., Na, J. C., & Chung, T. M. (2015). Detecting Ab-normal Behavior in SCADA Networks Using Normal Traffic Pattern Learning. InComputer Science and its Applications (pp. 121-126). Springer Berlin Hei-delberg.
6. Pramod, T. C., & Sunitha, N. R. (2013, July). An approach to detect malicious activities in SCADA systems. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on (pp. 1-7). IEEE.
7. Sousa, P., Bessani, A. N., Dantas, W. S., Souto, F., Correia, M., & Neves, N. F. (2009, June). Intrusion-tolerant self-healing devices for critical infrastructure protection. In Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on (pp. 217-222). IEEE.
8. Hayes, G., & El-Khatib, K. (2013, June). Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol. In Communications and Information Technology (ICCIT), 2013 Third International Conference on (pp. 179-184). IEEE.
9. Chen, Q., & Abdelwahed, S. (2014, April). Towards realizing self-protecting SCADA systems. In Proceedings of the 9th Annual Cyber and Information Security Research Conference (pp. 105-108). ACM.
10. 10. Blangenois, J., Guemkam, G., Feltus, C., & Khadraoui, D. (2013, Sep-tember). Organiza-tional Security Architecture for Critical Infrastructure. In Availability, Reliability and Securi-ty (ARES), 2013 Eighth International Con-ference on (pp. 316-323). IEEE.
11. 11. Ghosh D, Sharman R, Raghav Rao H, Upadhyaya S (2007) Self-healing systems—survey and synthesis. Decis Support Syst 42(4):2164–2185
12. 12. Panja, B., Oros, J., Britton, J., Meharia, P., & Pati, S. (2015, June). Intelligent gate-way for SCADA system security: A multi-layer attack prevention approach. In Computational Intel-ligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA), 2015 IEEE International Conference on (pp. 1-6). IEEE.
13. 13. A. Ameziane, A. Abou El Kalam, B. Bouhoula, R. Abbassi, A., Ait Ouahman, "Integrity-OrBAC: A new model to preserve Critical Infrastruc-tures Integrity". International Journal of Information Security, Springer, 2014, DOI 10.1007/s10207-014-0254-9

Slide title

Slide content

- Please **do not** alter the format of this template and do not exceed 15 slides

Important:

- Each paper has a 20-minute slot:
  - 15 min for presentation &
  - 5 min for questions and discussion

- Speakers are kindly required to respect the time limit