Some Security Problems and Aspects of the Industrial Internet of Things

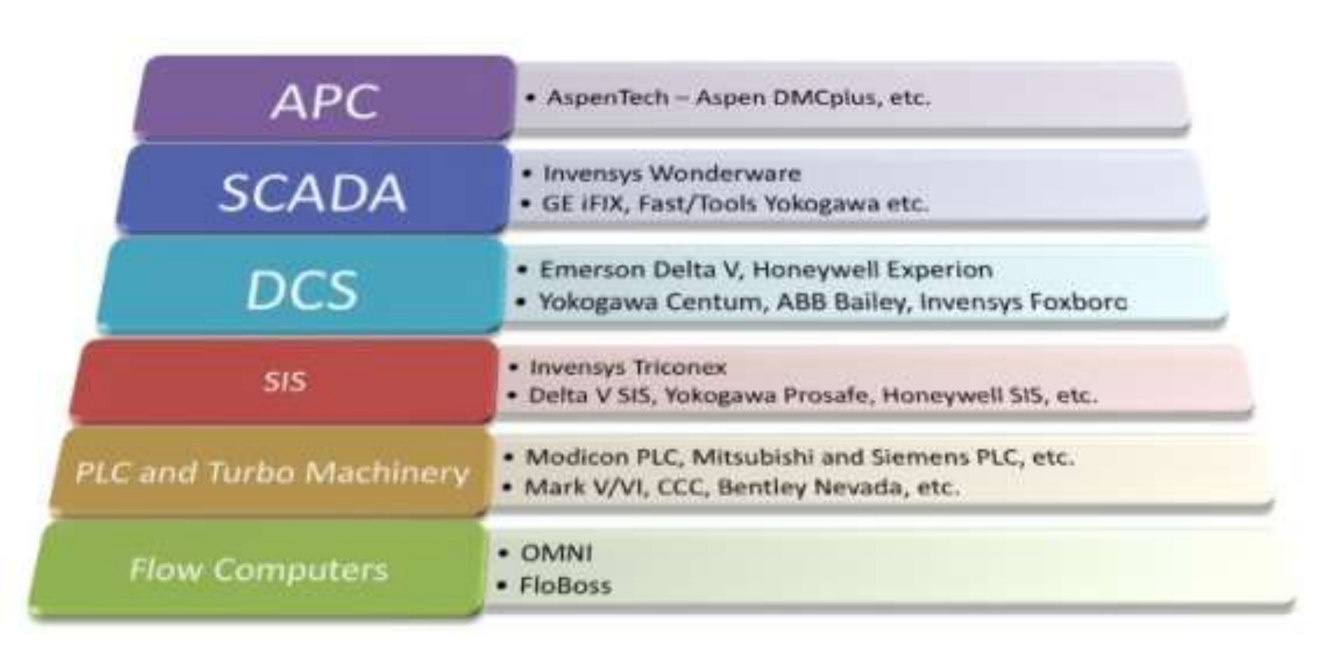
Georgi Tsochev

INTRODUCTION

Network and information security is crucial to computer networks and software applications. While the network security is a critical the requirement for the development of computer networks is a major disadvantage the methods of protection that can be easily implemented. There are many types of attacks and corresponding methods of protection.

IOT AND CYBER-PHYSICAL SYSTEMS

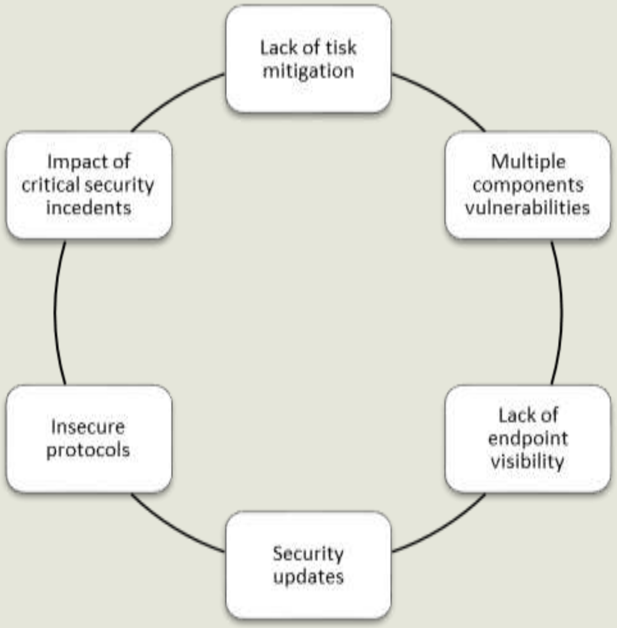
- Industry 4.0's technological foundation is based on intelligent, connected, embedded and digitally integrated systems that greatly assist the automation and autonomous management of production processes. Major role of the fourth industrial revolution are the Internet of Things (IoT) and Supervisory control and data acquisition (SCADA) systems.



APC	• AspenTech – Aspen DMCplus, etc.
SCADA	• Invensys Wonderware • GE iFIX, Fast/Tools Yokogawa etc.
DCS	• Emerson Delta V, Honeywell Experion • Yokogawa Centum, ABB Bailey, Invensys Foxboro
SIS	• Invensys Triconex • Delta V SIS, Yokogawa Prosafe, Honeywell SIS, etc.
PLC and Turbo Machinery	• Modicon PLC, Mitsubishi and Siemens PLC, etc. • Mark V/VI, CCC, Bentley Nevada, etc.
Flow Computers	• OMNI • FloBoss

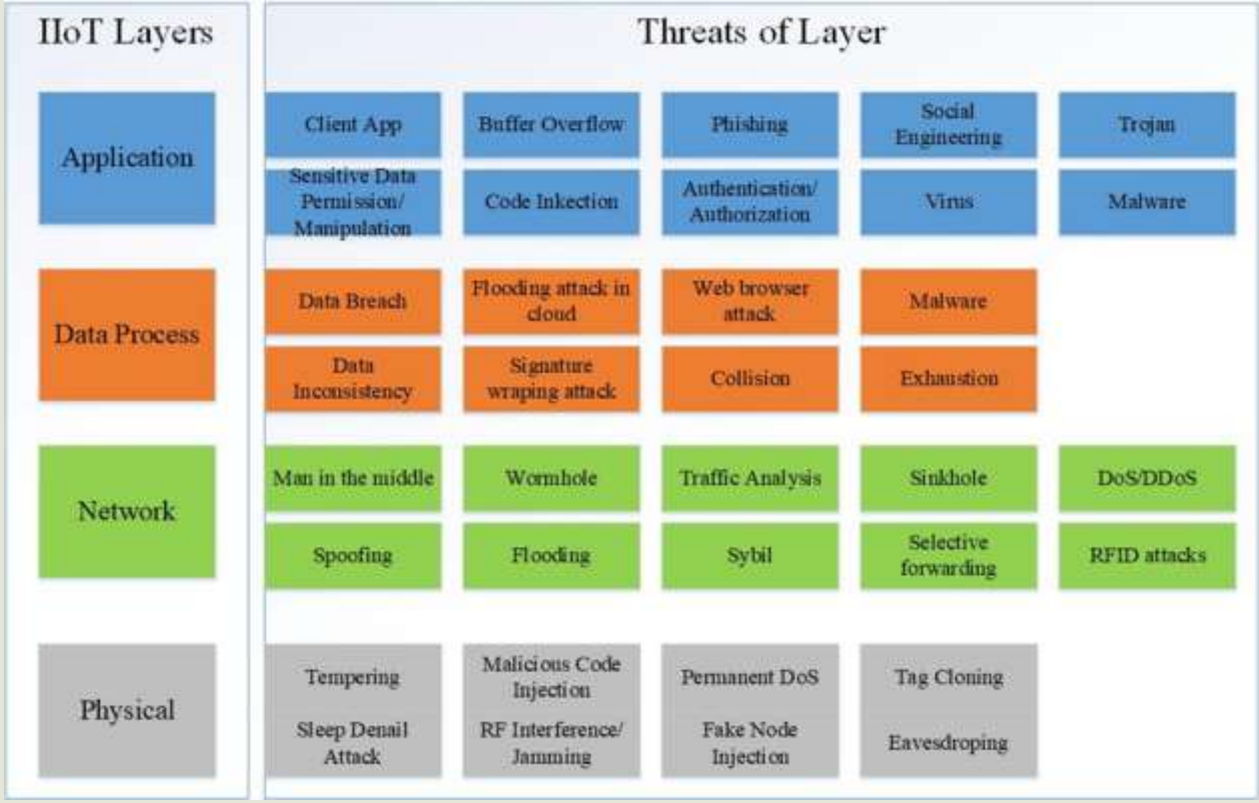
SOME SECURITY PROBLEMS

- The adoption of IIoT can change revolution in the work of industries, but there is the challenge to have strategies to strengthen efforts to digital transformation while maintaining security against the backdrop of increased connectivity.


Lack of tisk mitigation
Multiple components vulnerabilities
Lack of endpoint visibility
Security updates
Insecure protocols
Impact of critical security incedents

Analysis of the Problem

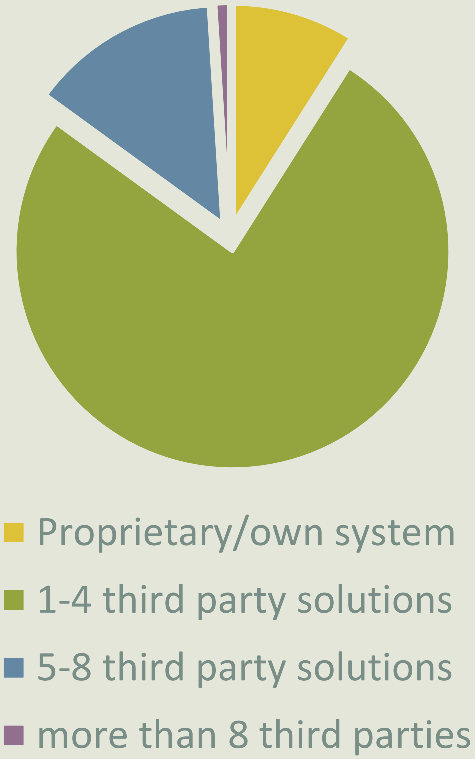
Based on a study, typical problems with the industrial Internet of Things can be defined as:



IIoT Layers	Threats of Layer				
Application	Client App	Buffer Overflow	Phishing	Social Engineering	Trojan
	Sensitive Data Permission/ Manipulation	Code Inkection	Authentication/ Authorization	Virus	Malware
Data Process	Data Breach	Flooding attack in cloud	Web browser attack	Malware	
	Data Inconsistency	Signature wraping attack	Collision	Exhaustion	
Network	Man in the middle	Wormhole	Traffic Analysis	Sinkhole	DoS/DDoS
	Spoofing	Flooding	Sybil	Selective forwarding	RFID attacks
Physical	Tempering	Malicious Code Injection	Permanent DoS	Tag Cloning	
	Sleep Denail Attack	RF Interference/ Jamming	Fake Node Injection	Eavesdroping	

Third party software / hardware based attacks

Considering the ecosystem of the Industrial Internet of Things, the most common attacks come from gaps from third party software / hardware.



CONCLUSION

- Given the various aspects of the industrialized Internet of Things and the possible security issues outlined above, it should be noted that there are three main lines that need to be addressed in symbiosis:
  - The organization must develop a vulnerability and risk management policy to deal with potential irregularities and must do this periodically
  - Implementation of endpoint security methodologies based on the secure-by-design approach
  - Use of tools for managing, detecting and identifying relevant industrial assets, including the use of IDPS monitoring and analysis systems and life cycle monitoring of different industrial actors
- Future work - As part of a project to study the security of cyber-physical connections in the context of computer networks using next-generation methods, this article provides a basis and beginning of the essential work to create a conceptual fashion for the protection of industrial systems
- **ACKNOWLEDGMENT**

This research is realized and funded under the scientific research project № 201ПР0010-09 “Investigating the security of cyber-physical connections in the context of computer networks through new generation methods” by the contract with TU-Sofia Internal Competition-2020.