



IIT KHARAGPUR



NPTEL ONLINE
CERTIFICATION COURSES

Advanced Technologies: Software-Defined Networking (SDN) in IIoT – Part 2

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

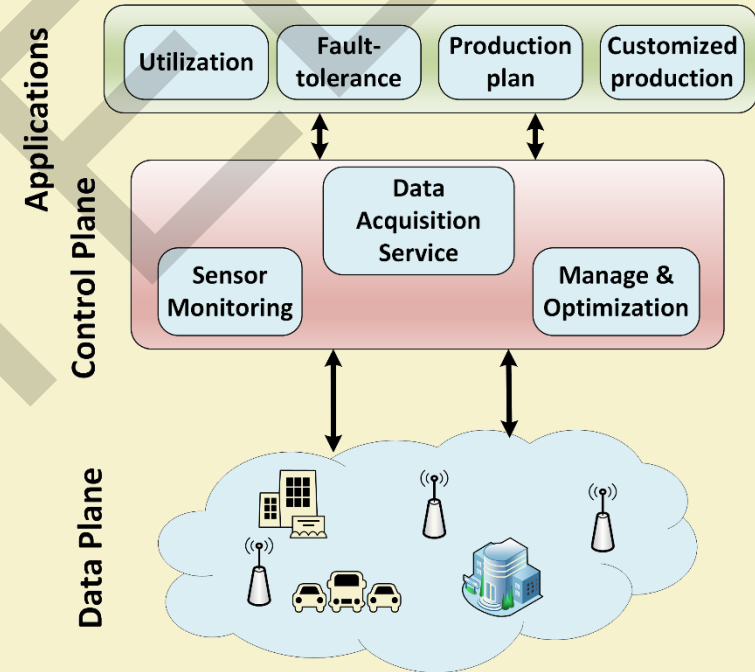
Research Lab: cse.iitkgp.ac.in/~smisra/swan/

SDIIoT Architecture

- SDIIoT – WSN
- SDIIoT – Public Networks
- SDIIoT – Industrial Cloud
- SDIIoT – Industrial bus & network

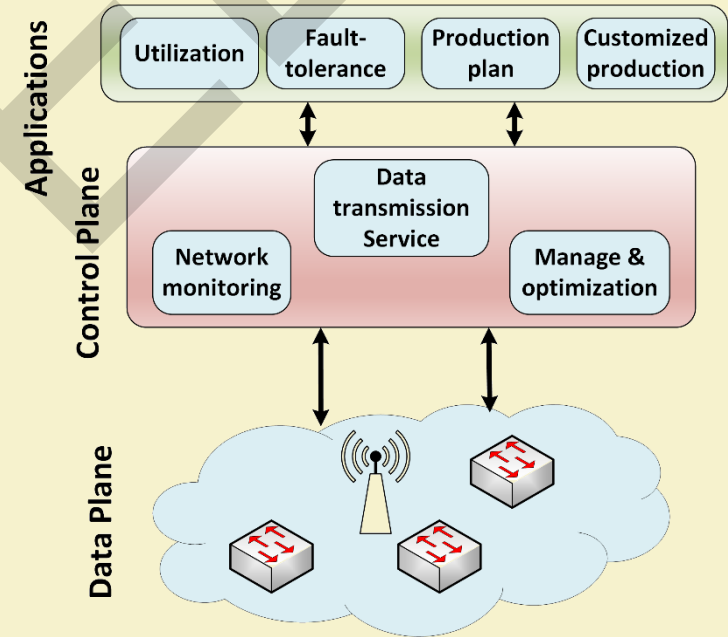
SDIIoT Architecture - WSN

- Software-defined WSN platform in the context of industry 4.0



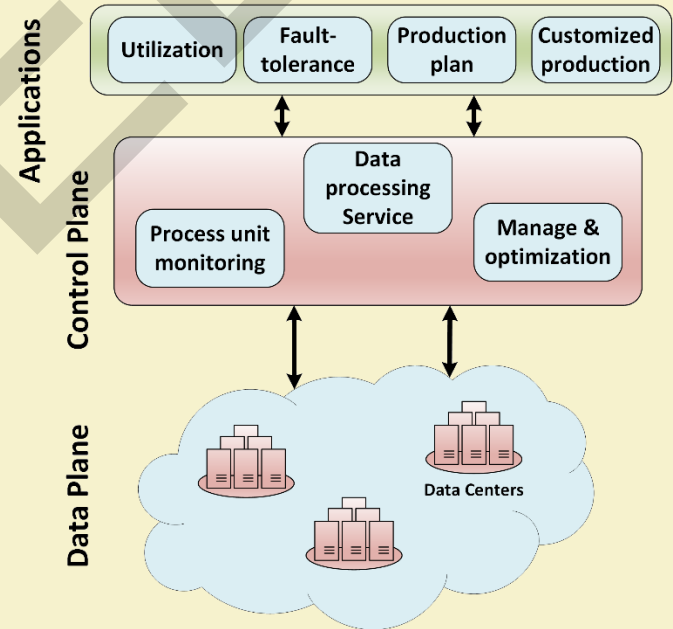
SDIoT Architecture – Public Networks

- Public network consists of switches, routers, and access network.
- Network monitoring, management and optimization are done at the control plane.



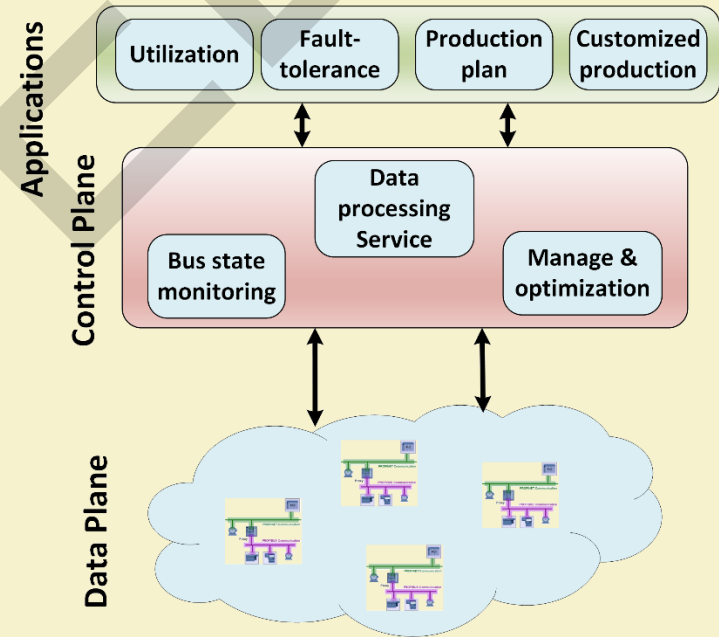
SDIIoT Architecture – Industrial Cloud

- Focuses on data center network.
- Data processing is done at this stage.



SDIIoT Architecture – Industrial Bus & Network

- It includes bus network.
- Monitoring of bus network is done.



Software-Defined 6TiSCH IIoT

- Time scheduled channel hopping (TSCH)
 - Deterministic communication
 - Efficient resource allocation in constrained networks (e.g., IoT and IIoT)
- IETF 6TiSCH is introduced to achieve the objectives

Challenges: SDN in 6TiSCH

- Unreliable link – low power and lossy network
- Control overhead due to message exchange between SDN controller and devices
- Increased jitter

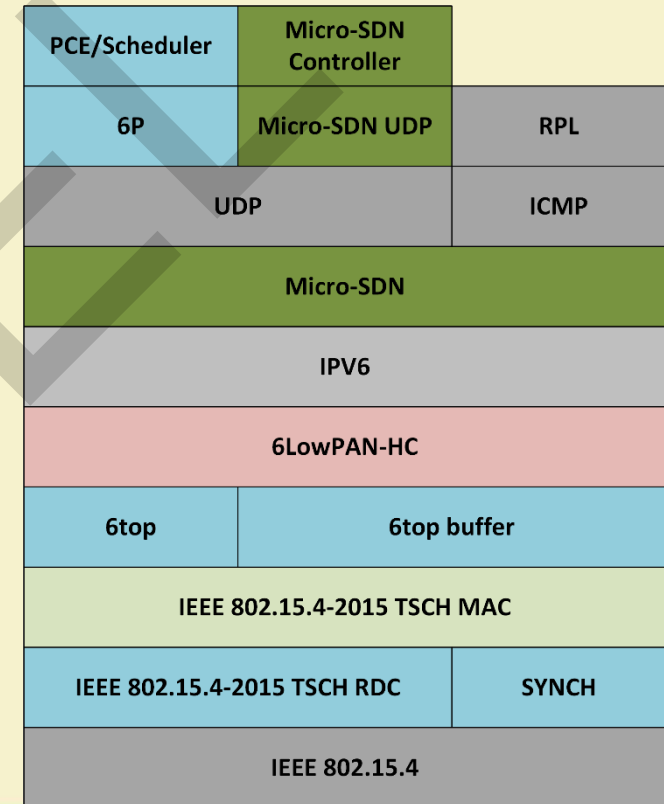
Software-Defined 6TiSCH*

- Slicing mechanism is proposed in Layer-2
- Dedicated forwarding paths across 6TiSCH network
- Slicing mechanism isolates the control overhead
- Allows deterministic and low-latency SDN controller communication
- Advantages of SDN is utilized, while minimizing the associated control overhead

*Baddeley et al., '17

SD-6TiSCH Protocol Stack

- μ SDN incorporates features for minimizing controller overhead
- Integrated with the Contiki IEEE 802.15.4-2015 stack



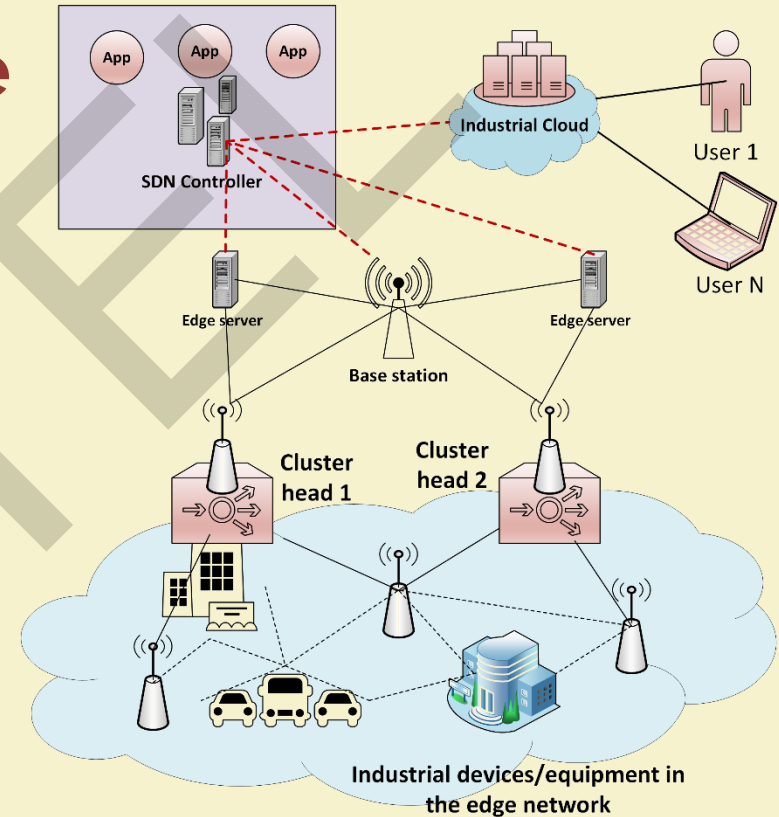
SD Edge Computing for IIoT*

- Adaptive transmission architecture with SDN and EC is proposed for IIoT
- Data stream is divided into two categories:
 - Ordinary data stream
 - Emergent data stream
- Emergent stream is served by finding paths which meet requirements based on a coarse-grained transmission path algorithm

*Li et al., '18

SD-Edge IIoT Architecture

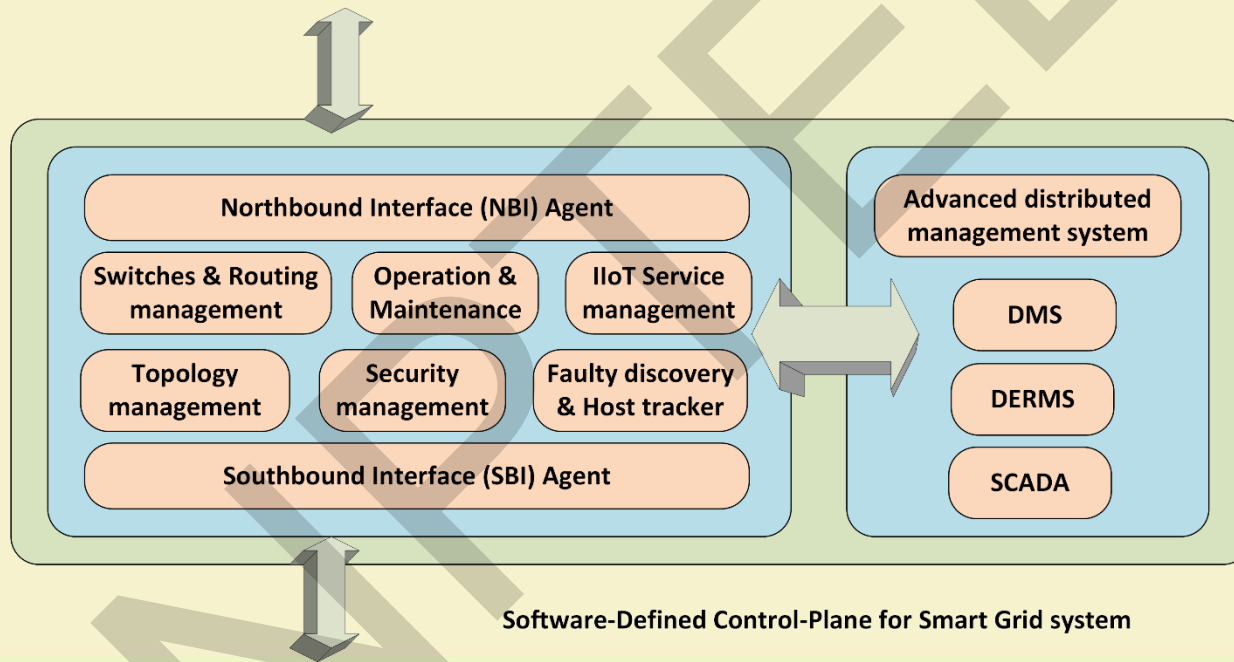
- Cluster head
- Industrial cloud
- Edge network
- SDN controller
- Devices/equipment
- Applications



Software-Defined Control Plane for Smart Grid*

- Smart grid monitoring system using a centralized controller
- Distribution management system (DMS)
- Distributed energy resource management system (DERMS)
- Supervisory control and data acquisition (SCADA)
- Presence of APIs at both ends – distribution side and generation side

*Al-Rubaye et al., '17



Challenges and Opportunities

- Absence of SDN protocol (like OpenFlow) for low power & lossy network
 - New protocol for enabling interaction between SDN controller and resource constrained devices may be proposed
 - Restructure of controller architecture and placement?
 - Do we need IoT middleware in software-defined IIoT system?

Challenges and Opportunities (contd.)

- Fog node/access devices play important role to provide emergent services (delay-constrained)
 - Can we utilize fog nodes as SDN controller?
 - What about the fault-tolerance of fog nodes?
 - Distributed/semi-distributed/fully centralized architecture?

References

- J. Wan, S. Tang, Z. Shu, D. Li, S. Wang, M. Imran, A. V. Vasilakos, "Software-defined industrial Internet of Things in the context of industry 4.0", *IEEE Sensors J.*, vol. 16, no. 20, pp. 7373-7380, Oct. 2016.
- M. Baddeley, R. Nejabati, G. Oikonomou, S. Gormus, M. Sooriyabandara, and D. Simeonidou, "Isolating SDN Control Traffic with Layer-2 Slicing in 6TiSCH Industrial IoT Networks", in Proc. of the *IEEE Conference on NFV-SDN*, 2017.
- X. Li, D. Li, J. Wan, C. Liu, and M. Imran, "Adaptive transmission optimization in sdn-based industrial internet of things with edge computing," *IEEE Internet of Things Journal*, 2018.
- S. Al-Rubaye, E. Kadhum, Q. Ni, A. Anpalagan, "Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency", *IEEE Internet of Things Journal*, 2017.

Thank You!!





IIT KHARAGPUR



NPTEL ONLINE
CERTIFICATION COURSES

Advanced Technologies: Security in IIoT – Part 1

Dr. Sudip Misra

Professor

**Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur**

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

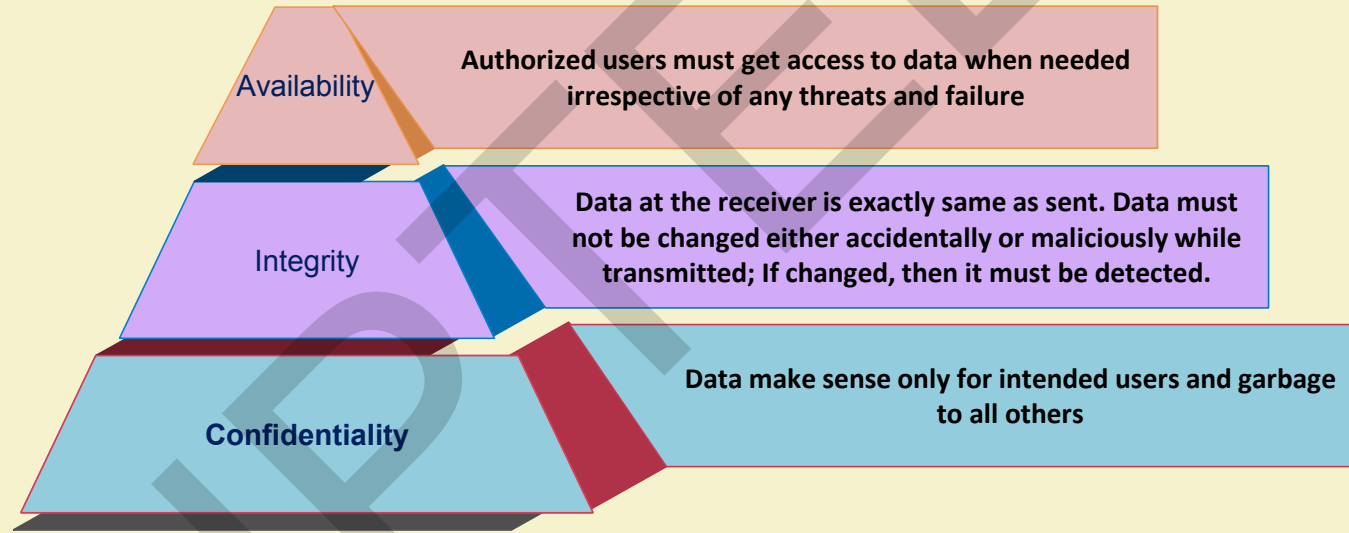
Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Need for IIoT Security

- Network of resource-constrained devices with low-bandwidth channels
- Devices with heterogeneous storage and processing capability
- Exposed to large attack surface
- Threats from hazards, device malfunctions and human errors
- Risks of Industrial accidents, disclosure of sensitive data and interrupted operations

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Basic Security Goals



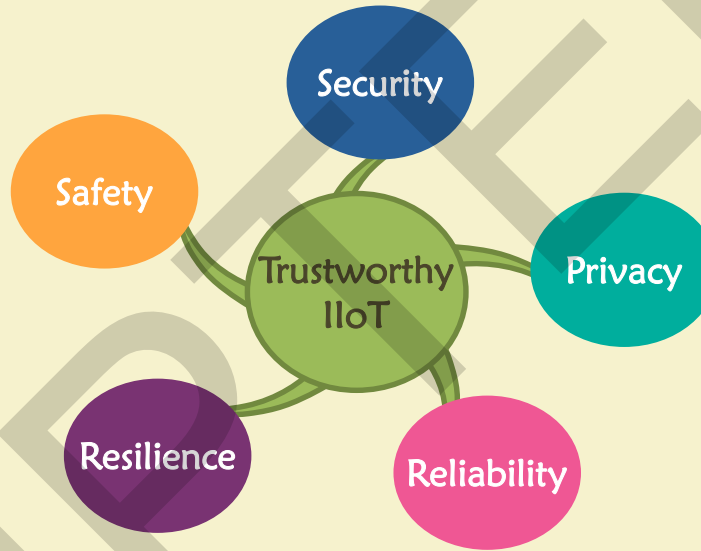
Source: "An Introduction to Information Security", NIST



Trustworthy IIoT

Safe operations of device and people without any risks and injury

Ability of the system to function correctly on dynamic adversarial conditions



Protecting the system from Unauthorized access, modification and destruction

Restriction on data access - who can access and by whom it can be disclosed

Ability of the system to perform under stated conditions correctly for the specified time period

Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium



Security In IIoT: Distinguished Aspects

- IIoT brings Information Technology (IT) and Operational Technology (OT) together
- Traditional security techniques working independently for IT and OT are no more applicable
- Simply integrating features from IT and OT is not possible
- Information security and device security
- Inadequate regulatory framework and standards.

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

IT and OT Security Requirement

- Current security architectures are mostly IT-centric
- Security assumptions for client-server model with well known communication protocols such as IP, TCP and HTTP.
- Assumes some well-known attacks and attack models
- OT systems only deploy legacy physical security protections
- Out-dated security protection for isolated OT networks
- Security for OT integrated with IT components ignored

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Cloud Complied IIoT Security Requirement

- OT infrastructure is controlled and managed at external networked cloud
- Data from thousands of devices stored in cloud
- Third-party services with trust-boundaries for security and privacy
- Safeguarding the control systems from incoming cloud information flow

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

IIoT Security Risk Management



Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

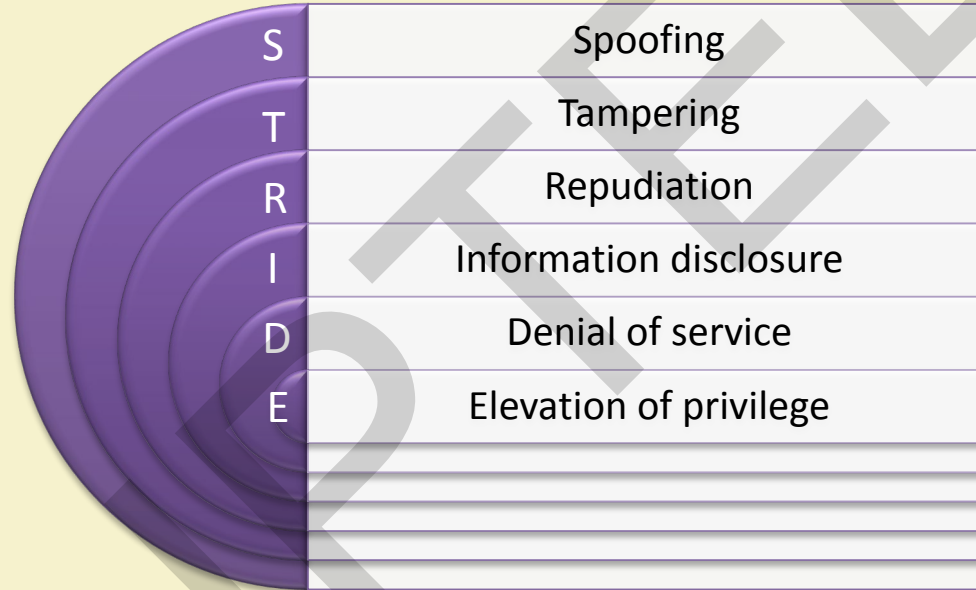


Classes of Attackers

- Outsourced firms
- Hardware vendors
- Third-party service providers like cloud vendors
- Internal unethical employees
- Organized crime groups

Source: “The who and how of cyber-attacks: types of attackers and their methods”, Out-law

STRIDE Threat Model

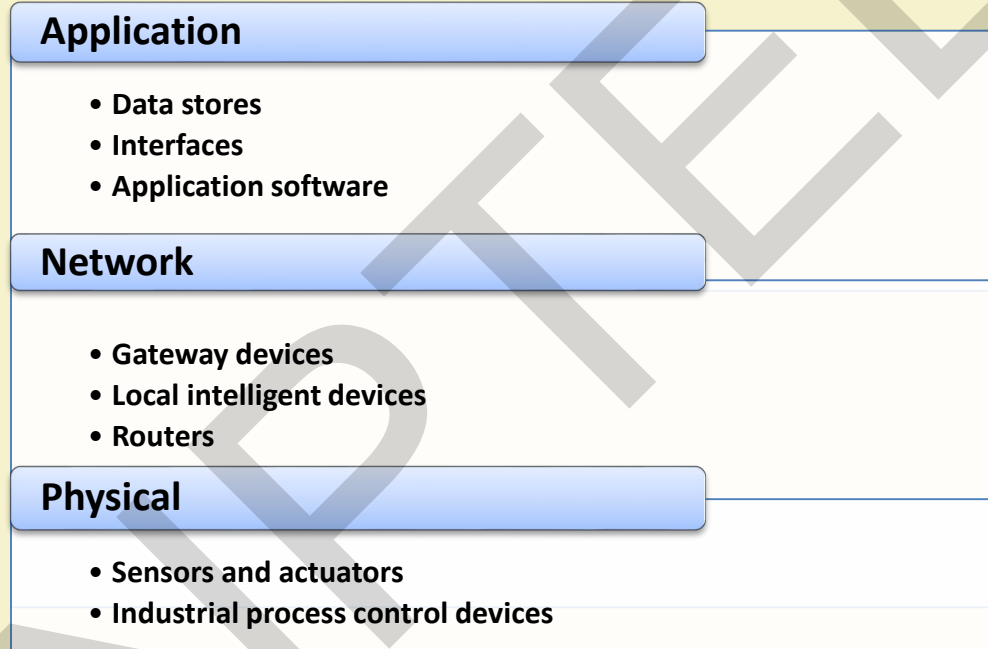
The diagram illustrates the STRIDE threat model. On the left, a purple semi-circular graphic contains the letters S, T, R, I, D, and E stacked vertically. To the right of this graphic is a table with six rows, each corresponding to a letter and a specific threat type.

S	Spoofing
T	Tampering
R	Repudiation
I	Information disclosure
D	Denial of service
E	Elevation of privilege

Source: "IoT Security Architecture | Microsoft Docs", Microsoft Azure



IIoT Attack Surface



Source: "IoT Attack Surface Areas", OWASP



IIoT Attack Vectors: Application Layer

- Data spoofing
- SQL injection
- DoS or DDoS
- Replay attack
- Resource exemption
- Reversal attack

Source: IoT Attack Surface Areas”, OWASP

IIoT Attack Vectors: Network Layer

- Traffic flooding
- Man-in-the-middle attack
- Misrouting
- Packet sniffing
- Resource exemption

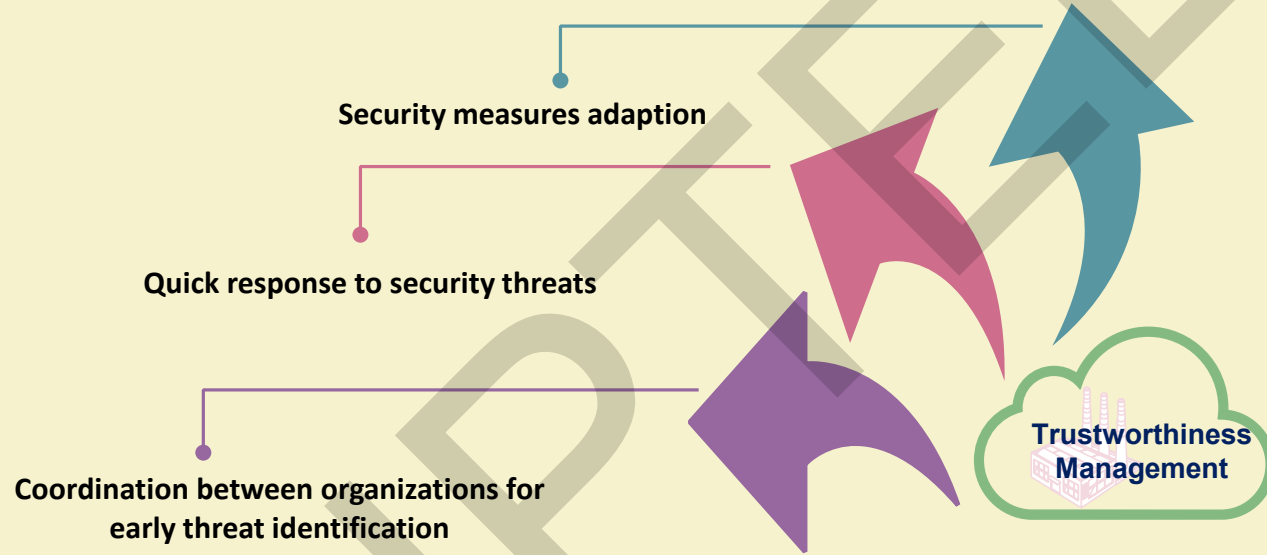
Source: IoT Attack Surface Areas”, OWASP

IIoT Attack Vectors: Physical Layer

- Impersonation attack
- Jamming attack
- Device tampering

Source: IoT Attack Surface Areas”, OWASP

Trustworthiness Management



Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

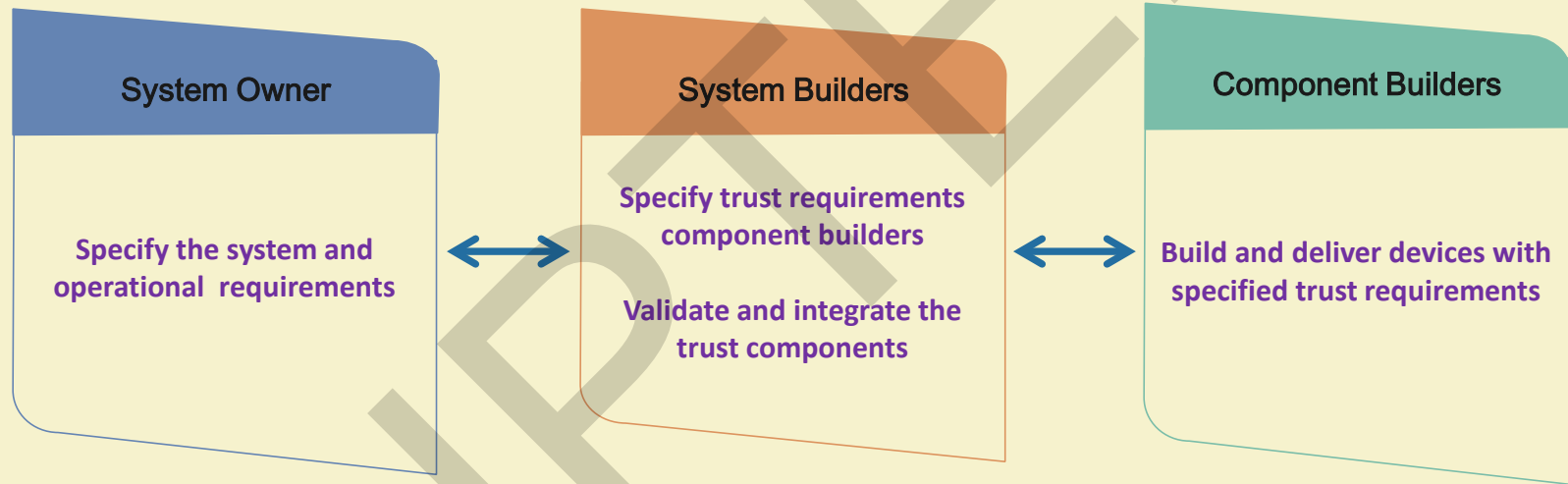


Trust Permeation in IIoT

- Hierarchical trust flow with in the IIoT system
- IIoT system consists of many units: design, development, manufacturing, logistics, etc.
- Trust permeation deals with trust establishment in all the components through the entire life cycle
- Device integrity and trustful chain of the devices make the whole system a secure one

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Trust Flow in IIoT System



Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium



Trust Functionalities: System Owner

- Every trust components are realized by the system owner
- The owner always ensures :
 - Trust requirements are met
 - The system works against the threats
 - Security patches and updates are implemented timely
 - Security risks are evaluated for further modifications

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Trust Functionalities: System Builder

- Feasibility of user requirement as per regulatory standards
- Design of a cost-efficient trustworthy system
- Trust requirements for every component and subcomponents
- Tests and certifications for component builder products
- Timely trust verification of devices and services

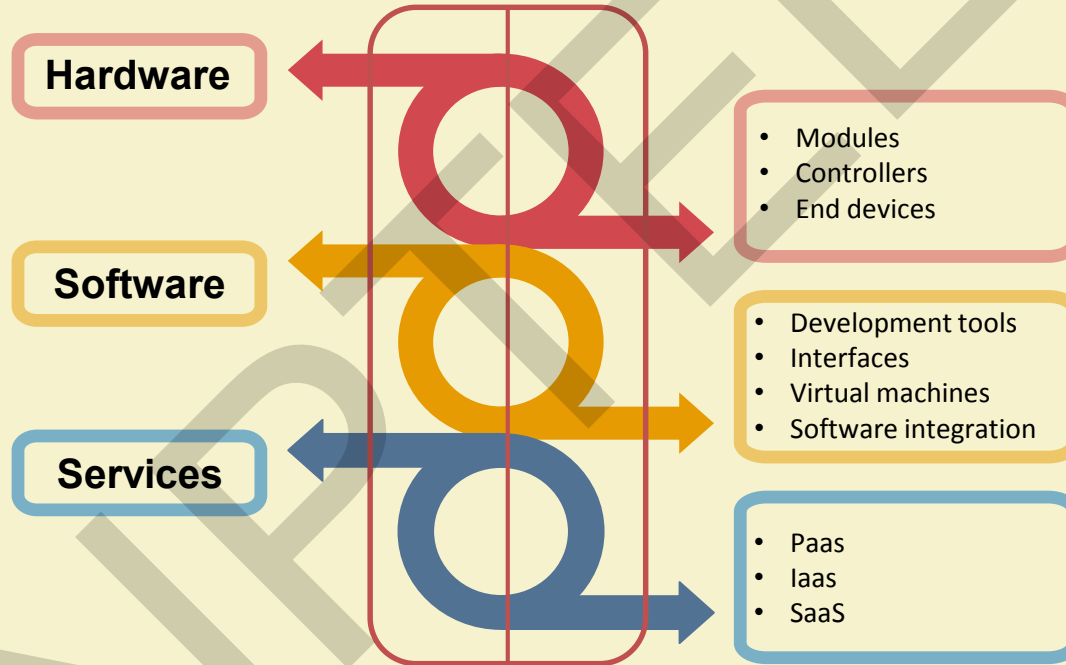
Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Trust Functionalities: Component Builder

- Hardware developers include trust requirements to devices and ensure trust compatibility with other components
- Software developers ensure security requirements with hardware compatibility and support for future updates
- Trust support for hardware or software replacements
- Trust support for different services

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Trust Functionalities: Component Builder (Contd.)



Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium



References

- [1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial Internet of Things: Challenges, Opportunities, and Directions”, *IEEE Transactions on Industrial Informatics*, 2018.
DOI :10.1109/TII.2018.2852491.
- [2] Z. Bakhshi, A. Balador, and J. Mustafa, “Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models”, *In proc. WCNC Workshop-2018*, Spain, 15-18 April, 2018.
- [3] “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium,
Available Online: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf, Accessed on Aug 20, 2018.
- [4] “Internet of Things Security Architecture: Security in IoT”, Microsoft,
Available Online: <https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture>,
Accessed on Aug 20, 2018.
- [5] “An Introduction to Information Security”, NIST, Available Online:
nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, Accessed on Aug 20, 2018.

References

- [6] “IoT Attack Surface Areas”, OWASP, Available Online: https://www.owasp.org/index.php/IoT_Attack_Surface_Areas, Accessed on August 20, 2018.
- [7] “The who and how of cyber-attacks: types of attackers and their methods”, Out-law, Available Online: <https://www.out-law.com/en/articles/2017/february/the-who-and-how-of-cyber-attacks-types-of-attackers-and-their-methods/> , Accessed on August 20, 2018.

Thank You!!





IIT KHARAGPUR



NPTEL ONLINE
CERTIFICATION COURSES

Advanced Technologies: Security in IIoT – Part 2

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

Security requirements for IIoT

- End-to-end security is the primary requirement of IIoT
- Both horizontal and vertical security are important
- Security of the whole system depends:
 - Security of deployed devices
 - Communication security
 - Data protection
 - Security management

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

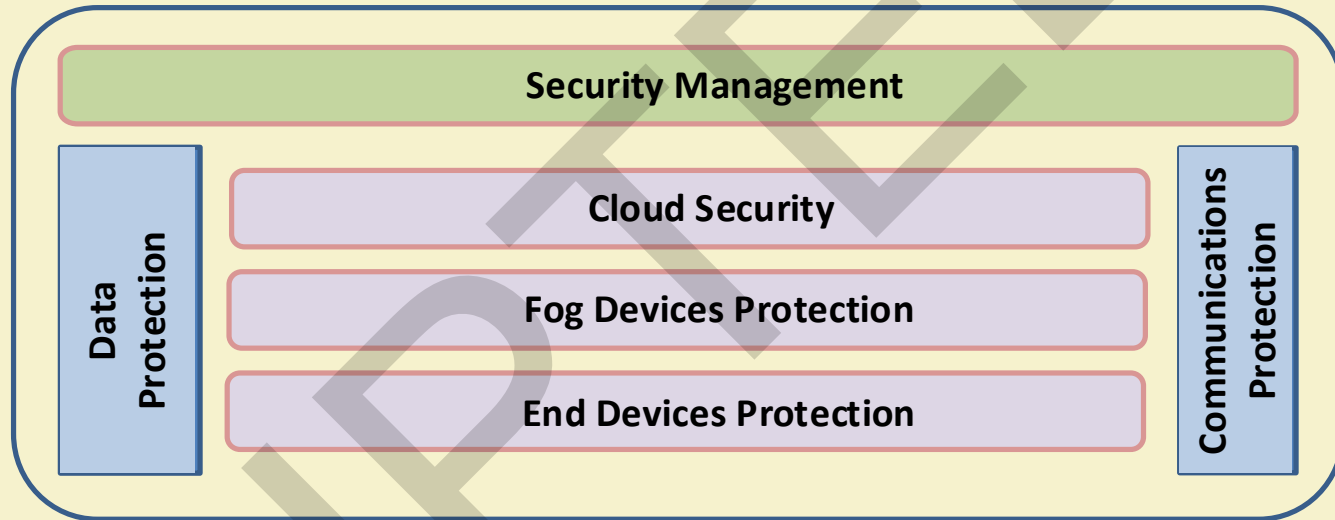


Security Framework for IIoT

- Every industrial application of IoT must have a security framework with its own requirements and solutions
- The framework should address:
 - Different security issues in IIoT
 - Trustworthy IIoT System
 - Major security building blocks of IIoT
 - Techniques for securing each independent block and secure integration

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

IIoT Security Building Blocks:



Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium and "Security for the Industrial Internet of Things", Accenture

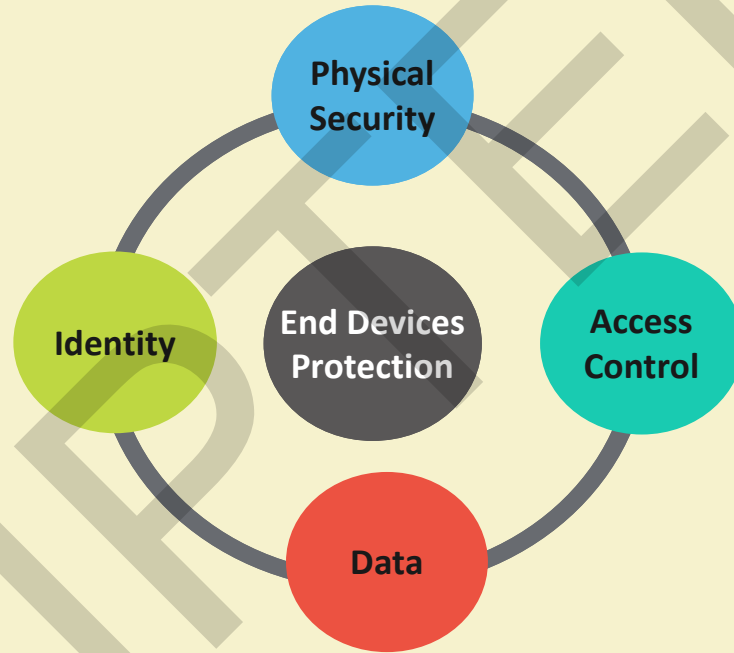


End Devices Protection - Challenges

- Devices: sensors, actuators, machines and many small embedded devices
- Resource constrained
- Many devices are mobile
- Heterogeneous
- No support for standard cryptographic protocols

Source: “Security for the Industrial Internet of Things”, Accenture

End Devices Protection - Requirement



Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium



End Devices Protection - Solutions

- Lightweight cryptographic protocols
 - Energy efficient authentication
 - Lightweight symmetric key cryptography
- IDS and behavior analysis at upper layer devices
 - Malicious behavior detection
 - Abnormal data traffic detection
 - Mitigation using proper actuation unit and signals

Source: Pacheco et al., 2017 and
“Lightweight Cryptography for the Internet of Things”, Sony Corporation

Fog Devices Protection

- Devices deployed near to end devices capable of notable computing and storage
- Requirements are same as end devices
- Standard cryptographic protocols for:
 - Authentication between fog devices
 - Authentication between fog devices and cloud
- Lightweight cryptography for security between for authenticating end devices

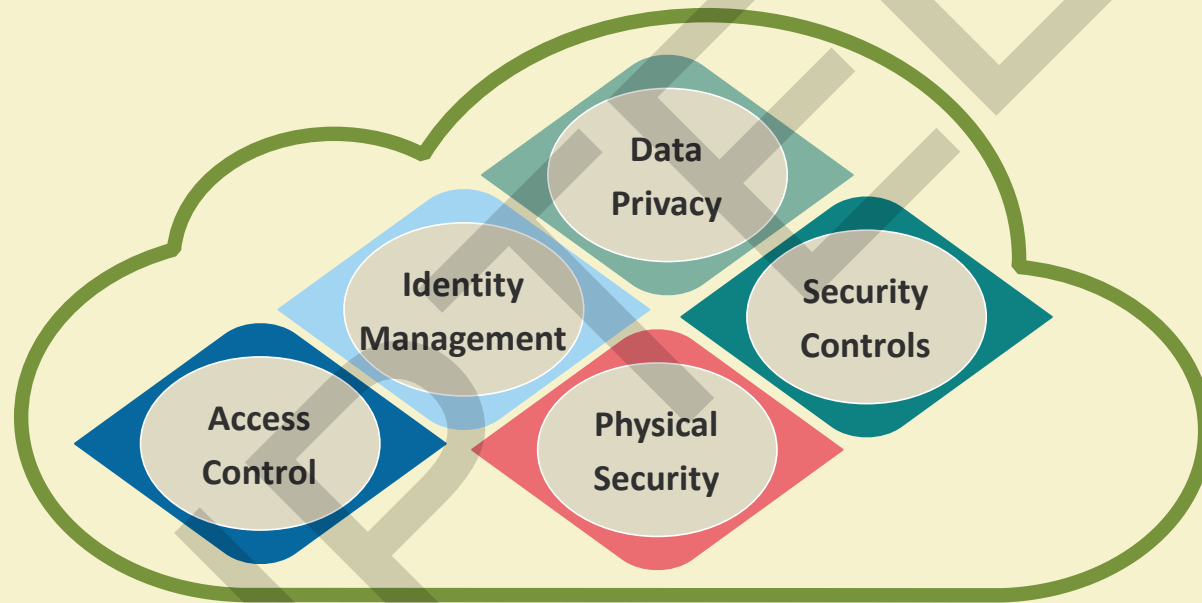
Source: Pacheco et al., 2017

Cloud Security

- Cloud is the data and control hub of the IIoT system
- Security requirement for :
 - Data protection
 - Applications
 - Cloud infrastructure
 - Limiting the service provider access
 - Access control for cloud resources

Source: "Cloud computing security", Wikipedia

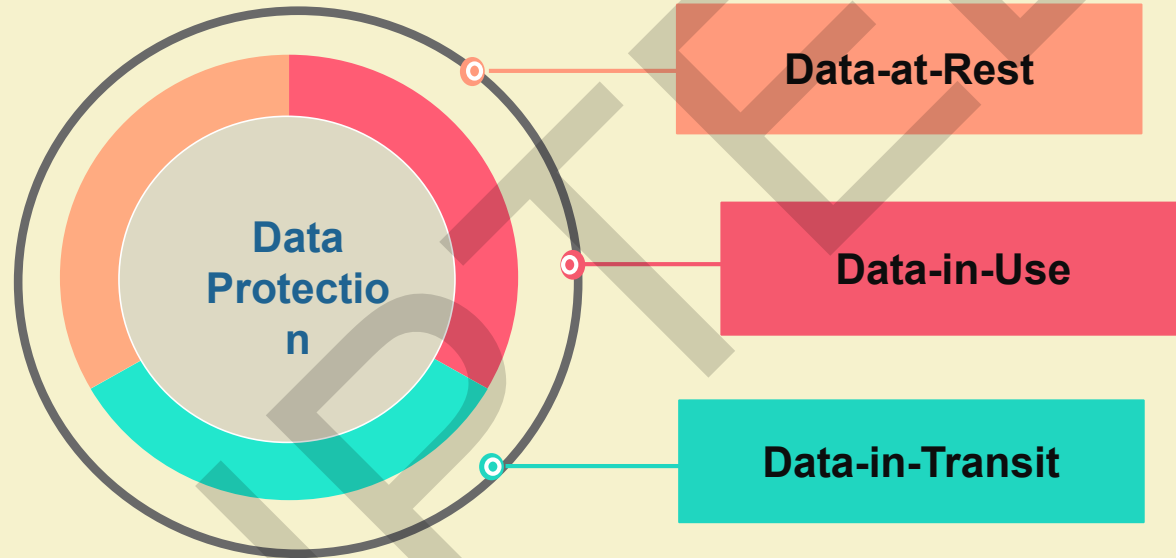
Cloud Security



Source: "Cloud computing security", Wikipedia,



Data Protection



Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium



Data Protection

- The most sensitive part of IIoT is data
- Different data sources and types with their own lifecycle, risks and security challenges
- Data protection includes:
 - Confidentiality
 - Integrity
 - Availability

Source: "An Introduction to Information Security", NIST

Communications Protection

- Secure exchange of information between IIoT devices
- Different security risk: sensor data, commands, actuation signals, log reports, configuration messages, etc.
- IIoT traffic and data formats are different from core network
- Protection involves:
 - Communication with devices at the same layer
 - Communication with devices at upper or lower layer

Source: Pacheco et al., 2017

Communications Protection Techniques

- Network access control
- Security gateways
- Network firewalls
- Cryptographic protocols with:
 - Strong mutual authentication
 - Authorization mechanism
 - Data ciphering

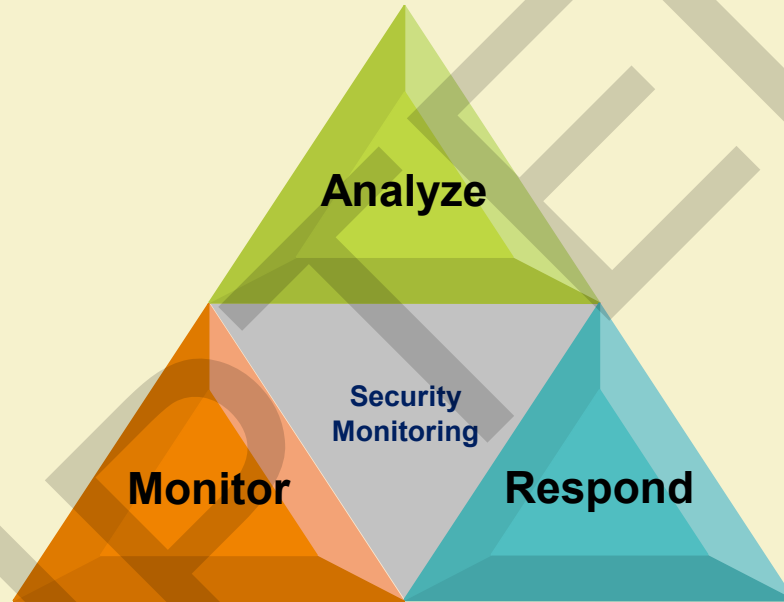
Source: Pacheco et al., 2017

Security Management

- Deals with configurations, periodic updates and managing the security controls
- An active unit, functions from establishment to end of entire IIoT system
- Prevention, detection, analysis and mitigation of security risks
- Performs security monitoring, policy management and updates over time as per standards

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

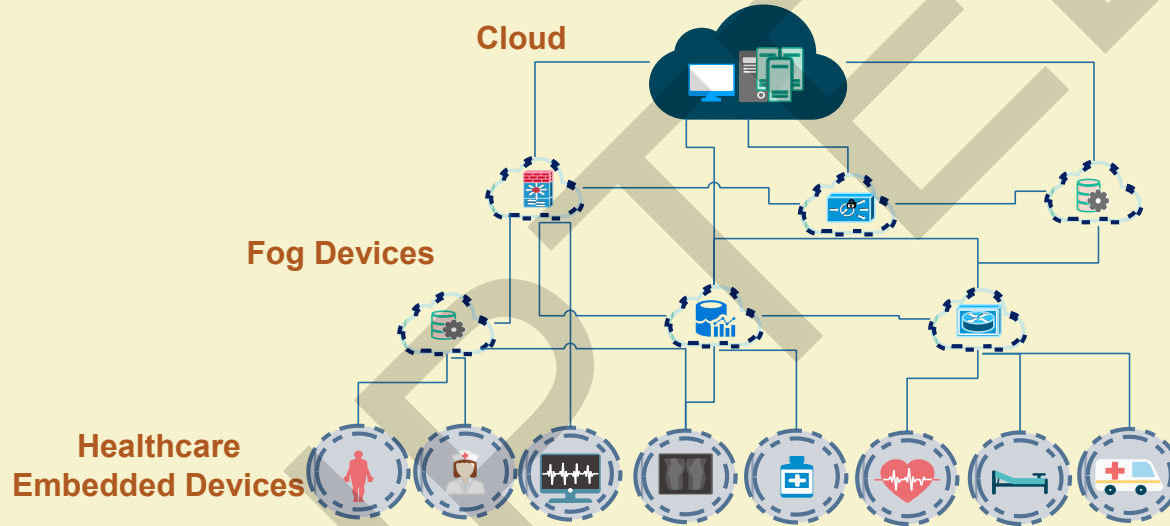
Security Monitoring



Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium



Use Case – Healthcare Industry



Source: Al-Joboury et al., 2017

Security in Healthcare IoT

- Devices security:
 - Protection of healthcare embedded devices
 - Protection of fog devices - gateways, processing units, data hubs
 - Cloud security
- Communications Security:
 - Healthcare devices - Fog devices (Lightweight cryptography)
 - Fog devices - Fog devices (Cryptography, Firewalls, Security gateways)
 - Fog devices - cloud (Cryptography, Security applications)

Source: Pacheco et al., 2017

Security in Healthcare IoT (Contd.)

- Data Protection:
 - Device data protection (Password, Signatures, Digital certificates)
 - Communication data (data ciphering and hashing)
 - Data at cloud (Access control lists, Signatures, Digital certificates)
- Security Management:
 - Global security handling at cloud
 - SDN-based security management and monitoring

Source: Pacheco et al., 2017 and Flauzac et al., 2017

Regulatory Standards for IIoT Security

- A security standard helps in achieving a common level of security in industries
- Standards help for manufacturers and vendors to offer services at different level of security
- For IIoT, security standards should include requirements of IT and OT
- Till date, there is no security standards specific to IIoT

Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

Standards Related to IIoT Security

IT Security

- ISO/IEC 154083: Common Criteria for Information Technology Security Evaluation
- ISO series of standards for privacy, framework and regulations
- ISO 27017, NIST SP 800-144, ENISA standard: Cloud security standards
- Common criteria and Federal Information Processing Standard (FIPS)

OT Security

- IEC 62443: Industrial automation and control systems security
- NIST SP 800-82: Security in Industrial Control Systems
- NERC-CIP: Critical infrastructure protection
- IEEE 1686: Standard for Intelligent Electronic Devices Cyber Security Capabilities
- NISTIR 7628: Guidelines for Smart Grid Cyber Security

Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

References

- [1] M. Katagi and S. Moriai, “Lightweight Cryptography for the Internet of Things”, Sony Corporation, Available Online: <https://iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf>, Accessed on 23 Aug, 2018.
- [2] J. Pacheco, D. Ibarra, A. Vijay, and S. Hariri, “IoT Security Framework for Smart Water Systems”, *In proc. Of IEEE/ACS 14th International Conference on Computer Systems and Applications*, 2017.
- [3] S. khan, S. Parkinson, and Y. Qin, “Fog computing security: a review of current applications and security solutions”, *Journal of Cloud Computing: Advances, Systems, and Applications*, vol. 6, no. 19, 2017.
- [4] I. M. Al-Joboury and E. H. Al-Hemiary, “F2CDM: Internet of Things for Healthcare Network Based Fog-to-Cloud and Data-in-Motion Using MQTT Protocol”, *In proc. of International Symposium on Ubiquitous Networking*, 2017.
- [5] Z. Bakhshi, A. Balador, and J. Mustafa, “Industrial IoT Security Threats and Concerns by Considering Cisco and Microsoft IoT reference Models”, *In proc. WCNC Workshop-2018, Spain, 15-18 April, 2018*.

References

- [6] “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium, Available Online: www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf, Accessed on Aug 20, 2018.
- [7] “Security for the Industrial Internet of Things”, Accenture, Available Online: <https://www.accenture.com/in-en/insight-security-industrial-internet-things>, Accessed on Aug 20, 2018.
- [8] “Securing the Internet of Things: A Proposed Framework”, Cisco, Available Online: <https://www.cisco.com/c/en/us/about/security-center/secure-iiot-proposed-framework.html>, Accessed on Aug 20, 2018.
- [9] O. Flauzac, C. González, A. Hachani, and F. Nolot, “SDN Based Architecture for IoT and Improvement of the Security”, *In proc. of 29th IEEE International Conference on Advanced Information Networking and Applications Workshops*, 2017.
- [10] “Cloud computing security”, Wikipedia, Available Online: https://en.wikipedia.org/wiki/Cloud_computing_security, Accessed on Aug 20, 2018.
- [11] “An Introduction to Information Security”, NIST, Available Online: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, Accessed on Aug 20, 2018.

Thank You!!





IIT KHARAGPUR



NPTEL ONLINE
CERTIFICATION COURSES

IIoT Applications: Factories and Assembly Line

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

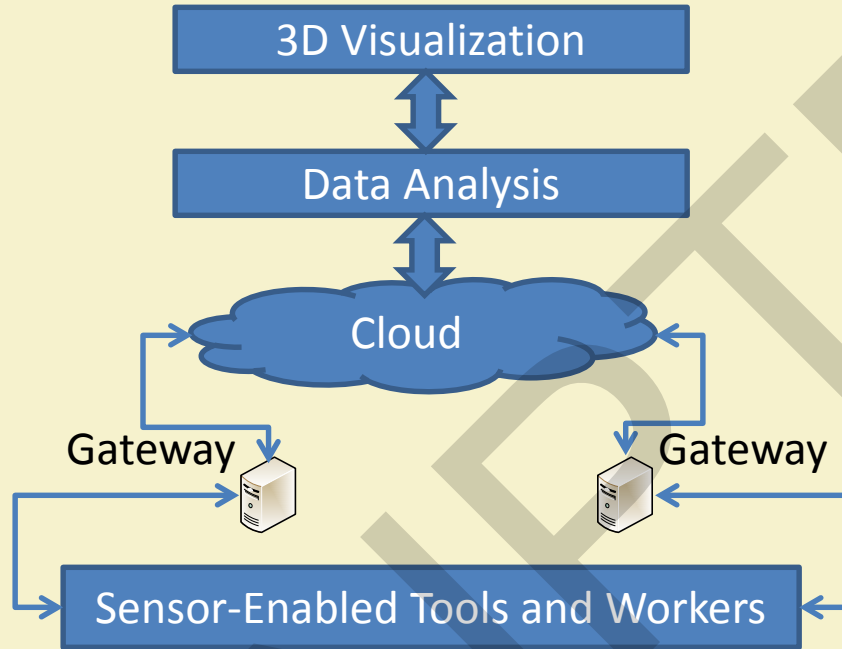
Traditional Manufacturing vs. Smart Manufacturing

- Challenges in Traditional Manufacturing
 - Unavailability of real-time data
 - Unbalanced workload
 - Longer changeover time
 - Extended production time

Smart Factory and Assembly Line

- **Smart Factory** involves machinery and equipment which improve processes through self-optimization and automation.
- **Benefits of Smart Factory:**
 - Supply of real-time data
 - Data analysis and quality control
 - Reduced changeover time
 - Reduced production time
 - Flexibility and easy management

Smart Factory



Overview of a Smart Factory

Features of a Smart Factory

- Connected
 - Continuous real-time data
- Optimized
 - Minimum manual intervention
- Transparent
 - Live metrics for quick decision
- Proactive
 - Prediction of future outcomes for taking preventive actions
- Agile
 - Flexibility and adaptability

Source: <https://www2.deloitte.com/insights/us/en/focus/industry-4-0/smart-factory-connected-manufacturing.html>

Smart Factory Applications: Airbus – Factory of the Future

- A European aircraft manufacturer
- Applies IoT technologies for production
- Collecting data on flights to improve in-flight experience
- Workers on factory floor use IoT-enabled devices
- Launched digital manufacturing initiative - Factory of the Future

Airbus: Factory of the Future

- Digital tracking and monitoring technology
- Tools and machines with integrated sensors
- Smart wearables
 - Industrial smart glasses
- 3D Real-time visualization of production process
- Deployed on the A330 and A350 final assembly lines in Toulouse
- Deployed for the A400M wing assembly operations in the UK

Smart Factory Applications: Kuka – IoT-Enabled Factory

- A German robotics maker
- Built an IoT-enabled factory
- The factory has hundreds robots
- Robots are connected with a private cloud
- 800 cars are produced per day

Smart Factory Applications: DeWalt – Construction Internet of Things

- A tool manufacturer
- Launched **Construction Internet of Things** initiative
 - Uses IoT Platform and Wi-Fi mesh network
 - Tracks workers and equipment
 - Monitors sites as large as an NFL football stadium

Smart Factory Applications: ABB - YuMi

- A power and robotics firm
- Operates across five continents
- Monitors robots via connected sensors
- Preventive maintenance
- YuMi Model
 - An initiative for collaboration between robots and humans

Smart Factory Applications: Amazon – Robotic Shelves

- An e-commerce company
- Uses robotic shelves
 - Robots carry and rearrange shelves
 - Automated product search
 - Robots locate and bring shelves to workers
- In 2014, the operating cost was cut down by 20% after using robotic shelves

Smart Factory Applications: Caterpillar – AR App

- A heavy-equipment maker
- Uses Augmented Reality (AR) with IoT
- AR app generates end-to-end view of the factory floor
- Machine operators detect need for tool replacement after viewing the end-to-end view
- AR app sends instructions for tool replacement

Caterpillar: IoT-Driven Ship Maintenance

- The marine division uses shipboard sensors to perform **Predictive Maintenance Analytics**
- The sensors monitor generators, engines, GPS, air conditioning systems and fuel meters.
- Analysis of the sensed data provides some useful insights
 - The power usage of refrigerated containers is linked with fuel meter readings
 - The cost of hull cleaning is correlated to performance enhancement
 - Optimized cleaning schedule saves up to \$400,000 per ship

Caterpillar: Predictive Maintenance Analytics

- A machine learning technique
- Uses R, Python, and Weka
- Easier fault-correction
- Reduced downtime
- Increase profitability

Smart Factory Applications: Fanuc – Zero Downtime System

- A robotic maker
- Uses predictive maintenance to reduce downtime
- Cloud-based analytics with in-built sensors
- Predicts component failure
- The Zero Downtime (ZDT) system is the winner of the GM Supplier of the Year Innovation Award 2016

Smart Factory Applications: Gehring – Connected Manufacturing

- Makes honing machines
- Uses cloud-based analytics
- Sends real-time data of new machines to customers to confirm requirements before order placement
- Optimizes productivity

Smart Factory Applications: Hitachi - Lumada

- Offers IoT platform – Lumada
- Five layers
 - Edge
 - Core
 - Analytics
 - Studio
 - Foundry

Smart Factory Applications: Maersk – Intelligent Shipping

- A container shipping company
- Tracks assets and fuel consumption using sensors
- Uses IoT for preserving refrigerated containers
- Uses blockchain technology for supply chain optimization

Smart Factory Applications: Magna Steyr – Smart Packaging

- An automotive manufacturer
- Uses IoT for tracking assets including tools and vehicle parts
- Smart packaging
 - Bluetooth-enabled packaging
 - Tracks components in warehouses
- Employees use wearable technologies

Magna Steyr: Driverless Transport System

- Digital factory
 - A virtual image of entire factory is created
 - Virtual image provides real-time control and detects anomaly
- 3D map of digital factory
 - Driverless transport vehicles follow the 3D map to move parts along the assembly line
- IoT-based predictive maintenance
 - Data sensed by driverless transport vehicles are analyzed in cloud to detect deviations

Smart Factory Applications: North Star BlueScope Steel – IoT for Worker Safety

- A major supplier in steel industry
- Attached wearables to helmets and wristbands
- Wearables send health parameters to supervisors
- Supervisors give break to overloaded workers
- Sensors monitor environmental parameters to detect radiation and toxic gases

Some Other Smart Factory Applications

- Rio Tinto: IoT for mining
 - Driverless trucks and trains to pull ore from mining sites
 - Autonomous drill technology
- Real-Time Innovations: microgrid technology
 - Divides a power grid in to multiple distributed microgrids
- Bosch: Track and Trace Testbed
 - Locates handtools and shows specific requirements for each tool
 - Save labour and reduces errors

References

- [1] <https://www.ioti.com/industrial-iiot/top-20-industrial-iiot-applications>
- [2] <https://internetofbusiness.com/9-examples-manufacturers-iiot/>
- [3] <https://www.softwebsolutions.com/resources/production-line-monitoring-solution.html>
- [4] <https://internetofbusiness.com/iiot-helping-airbus-make-planes-better/>
- [5] <https://www.ioti.com/industrial-iiot/software-deals-take-center-stage-europes-industrial-fair>
- [6] <https://www.ioti.com/industrial-iiot/dewalt-build-iiot-construction-platform-mesh-network>
- [7] <https://www2.deloitte.com/insights/us/en/focus/industry-4-0/smart-factory-connected-manufacturing.html>
- [8] <https://www.kuka.com/en-in>
- [9] <https://new.abb.com/>
- [10] <https://www.technologyreview.com/s/538601/inside-amazons-warehouse-human-robot-symbiosis/>
- [11] <https://www.forbes.com/sites/bernardmarr/2017/02/07/iiot-and-big-data-at-caterpillar-how-predictive-maintenance-saves-millions-of-dollars/#8e6f5c772409>

References

- [12] <https://www.fanuc.com/>
- [13] <https://www.gehring.de/en-ww>
- [14] <https://www.hitachivantara.com/en-in/products/internet-of-things/lumada.html>
- [15] <https://www.maerskline.com/>
- [16] <https://www.magna.com/company/company-information/magna-groups/magna-steyr>
- [17] <http://nsbsl.com/>
- [18] <https://www.riotinto.com/>
- [19] <https://www.rti.com/>
- [20] [https://www.ioti.com/industrial-iiot/iic-testbeds-take-iiot-use-cases-out-lab-and-real-world](https://www.ioti.com/industrial-iot/iic-testbeds-take-iiot-use-cases-out-lab-and-real-world)

Thank You!!





IIT KHARAGPUR



NPTEL ONLINE
CERTIFICATION COURSES

IIoT Applications: Food Industry

Dr. Sudip Misra

Professor

Department of Computer Science and Engineering

Indian Institute of Technology Kharagpur

Email: smisra@sit.iitkgp.ernet.in

Website: <http://cse.iitkgp.ac.in/~smisra/>

Research Lab: cse.iitkgp.ac.in/~smisra/swan/

IoT and Food Industry

- Sensing layer
 - Networked sensors monitor food quality along the supply chain
 - WSNs monitor environmental conditions
- Communication layer
 - Stakeholders access supply chain data
- Application layer
 - Applications for farmers, retailers, government, analysts, and consumers

IoT and Food Industry: The Future

- Sensors monitor humidity, temperature, and composition of food products
- Real-time data analysis
- Easier process control and increased food safety
- A rice packet can be traced back to the paddy field

Impacts of IoT in Food Industry

- Efficient production line
 - IoT monitors equipment performance
 - Detects anomaly in production line
 - Real-time solutions by predictive maintenance
- Food safety
 - Temperature tracking sensors
 - Automated Hazard Analysis and Critical Control Points (HACCP) checklists

Impacts of IoT in Food Industry

- Transparency of the supply chain
 - Availability of real-time data about products
 - Easier to find inefficiencies
 - Easier to meet food safety regulations
- Less wastage
 - Analysis of real-time information of food products reduce food wastage

Applications of IoT in Food Industry: On the Farm

- Sensors monitor weather, crop maturity, and presence of insects
- Soil moisture sensors optimize irrigation and fertilization

Applications of IoT in Food Industry: In the Livestock Barns

- Sensors monitor health parameters of animals
- Automated feeding cycles
- Diet control
- Automated temperature control in brooding barns and hatchery

Applications of IoT in Food Industry: On Equipment

- GPS tracking
- Drone-assisted field monitoring

Applications of IoT in Food Industry: For Maintenance

- Embedded sensors monitor machine performance
- Early detection of warning signs
- Smart maintenance extends equipment lifetime

Applications of IoT in Food Industry: To Improve Margins

- Predictive analysis
- Spotting early warning signs
- Well informed decisions
- Profit maximization

Applications of IoT in Food Industry: For the Consumer

➤ SmartLabel

- An initiative by the Grocery Manufacturers Associations (GMA)
- Uses QR code to provide product related information to consumers
- Provides ingredient details, allergens exposure, nutrition value, and many more

Applications of IoT in Food Industry: About the Product

- Consumers scan QR code to access product information
- Product information includes nutrition, ingredients, allergens, third-party certifications, social compliance programs, usage instructions, advisories & safe handling instructions, etc.

Applications of IoT in Food Industry: In the Factory

- Connected processes and workers
- Insights gained from IoT technology help to improve quality
- Reduction in time to market (TTM)

Applications of IoT in Food Industry: About Compliance and Safety

- IoT insights help to identify and isolate unsafe food
- Timely action for food quality and safety issues
- Increases confidence of food manufacturers

Applications of IoT in Food Industry: For Empowering the Workers

- Safety glasses and other wearables
- Increases productivity and efficiency

IoT Solutions for Food Industry: CityCrop – Intelligent Indoor Garden

- Provides intelligent indoor garden to grow fruits, herbs, vegetables, greens, and edible flowers
- Climate control
- Live monitoring
- Smart notifications
- Plant doctor

IoT Solutions for Food Industry: Diagenetix - BioRanger

- Detects the presence of microbial disease in food
- BioRanger
 - A small handheld device
 - Connects with android app
 - Instantly detects pathogens in food

IoT Solutions for Food Industry: Eskesso – The Cooking Sorcery

- Wifi-connected smart cooking device
- Easy monitoring of cooking status via smartphone app
- Smart cooking
 - By placing food packet and Eskesso device in a pot of water, selecting the recipe and starting via smartphone app

IoT Solutions for Food Industry: Culinary Science Industries – Flavor Matrix

- Infuses foods and beverages with unique flavors
- Collects data on food ingredients
- Collects user data
- Uses machine learning and data analysis to enhance flavor of dishes and provide user specific food and beverage pairing

IoT Solutions for Food Industry: Intellicup – Smart Cups

- Smart beverage vending
- Reduces waiting time and increases profit at beverage shops
- IoT-enabled cups
 - Integrated NFC chip at the cup base
 - Connects cups to mobile banking platform and IntelliHead – a modular dispensing unit
 - NFC chips connects each user to a cup
 - Cups are reusable and made with biodegradable material

IoT Solutions for Food Industry: Intellicup – Smart Cups

- How the smart cups work
 - Separate apps for merchants and customers
 - Customers create Intellicup accounts using the app
 - Transferring fund to e-wallets
 - Linking cup to the e-wallet by scanning a QR code via the app
 - Docking the cup on the dispensing unit (Intellihead)
 - Customers enjoy the beverage

Some Other IoT Solutions for Food Industry

- Spinn Inc.: smart coffee brewing machines
 - Connects coffee brewing machines with Amazon Echo
 - Auto-order feature
- FarmShelf: smart indoor farming
 - IoT-enabled climate control for growing crops
 - Automatic notification regarding crop status

References

- [1] <https://sealedair.com/blog/3-ways-iot-transforming-food-industry>
- [2] www.buhlergroup.com/global/en/about-buehler/media/core-topics/internet-of-things.htm
- [3] <https://www.comparethecloud.net/articles/how-internet-of-things-transforming-food-industry/>
- [4] <http://blogs.infor.com/manufacturing-matters/2018/04/top-ten-iot-applications-food-beverage-industry.html>
- [5] <https://www.gmaonline.org/issues-policy/health-nutrition/smartlabeltm-consumer-information-transparency-initiative/>
- [6] <https://www.disruptordaily.com/top-10-internet-things-companies-watch-food-industry/>
- [7] <https://www.citycrop.io/>
- [8] <http://diagenetix.com/>
- [9] <http://www.eskesso.com/en/home-cf/>
- [10] <http://culinaryscienceindustries.com/>

References

- [11] <https://www.spinn.com/>
- [12] <http://intellicup.com/>
- [13] <http://farmshelf.co/>

Thank You!!

