IIT KHARAGPUR

NPTEL ONLINE
CERTIFICATION COURSES

NPTEL

# Advanced Technologies: Security in IIoT – Part 1

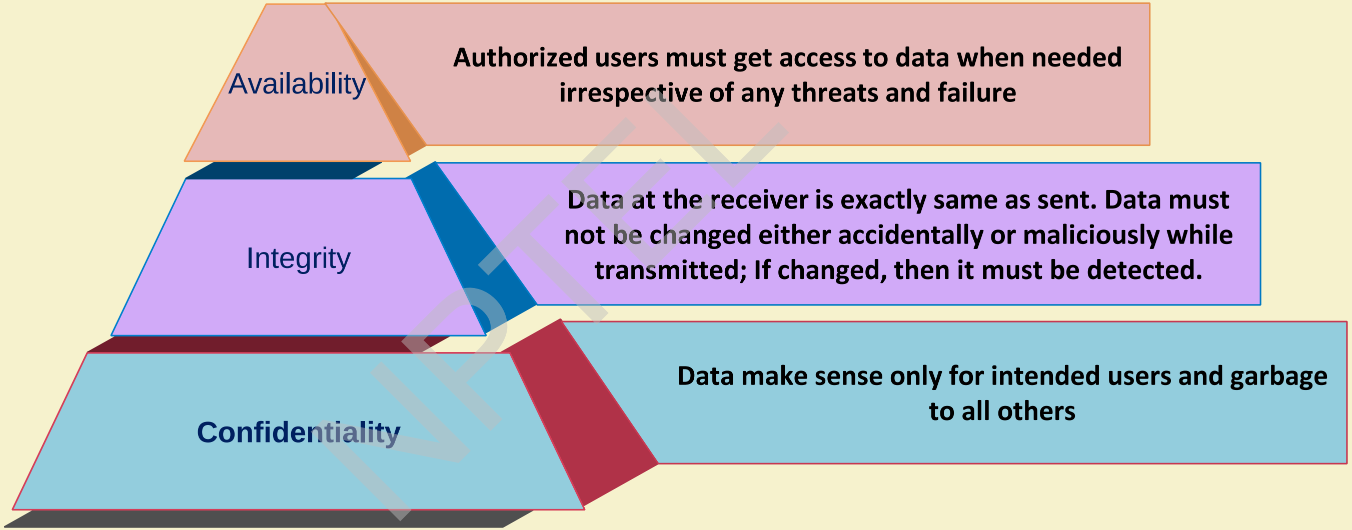
Dr. Sudip Misra
Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Email: smisra@sit.iitkgp.ernet.in
Website: http://cse.iitkgp.ac.in/~smisra/
Research Lab: cse.iitkgp.ac.in/~smisra/swan/

# 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



Authorized users must get access to data when needed irrespective of any threats and failure

Data at the receiver is exactly same as sent. Data must not be changed either accidentally or maliciously while transmitted; If changed, then it must be detected.

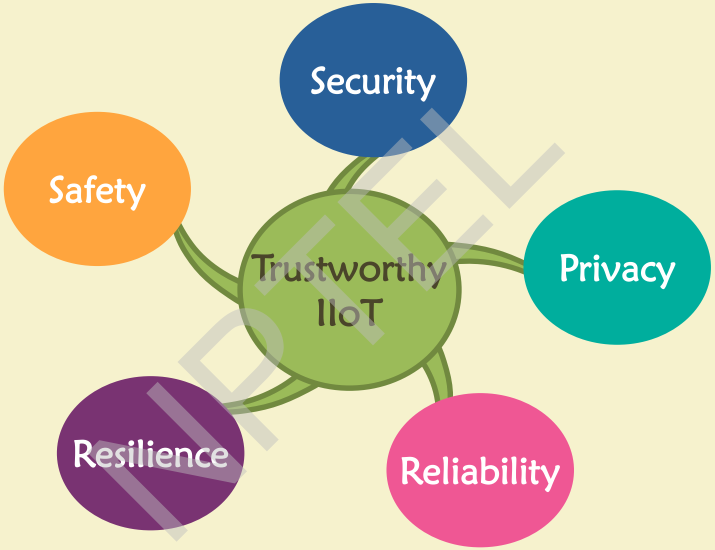
Data make sense only for intended users and garbage to all others

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

- 01 Avoiding risks
- 02 Mitigating risks
- 03 Outsourcing risks
- 04 Accepting risks
- 05 Balancing residual risks

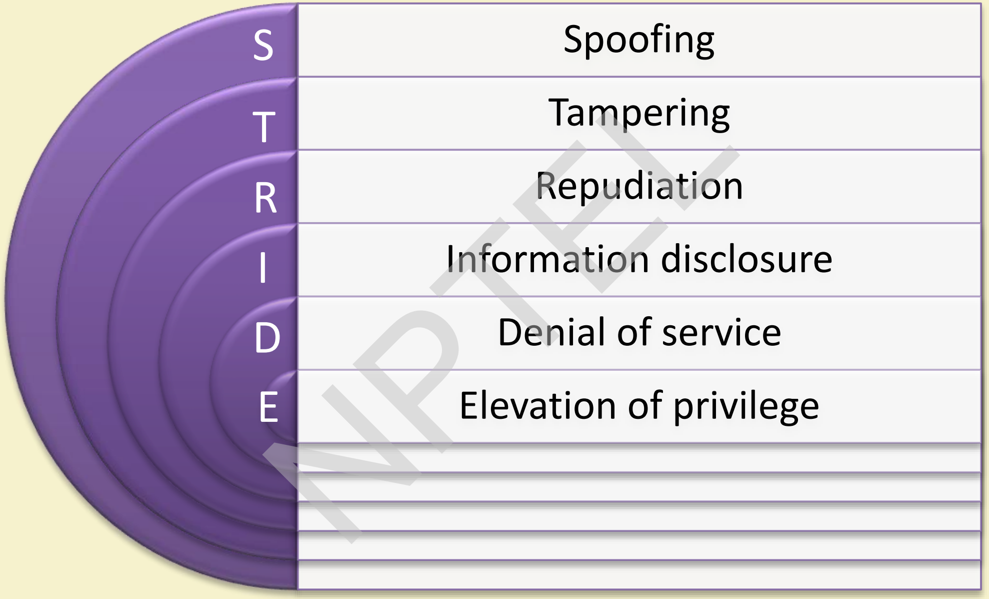
Source: “Industrial Internet of Things Volume G4: Security Framework”, Industrial Internet Consortium

# 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



S Spoofing

T Tampering

R Repudiation

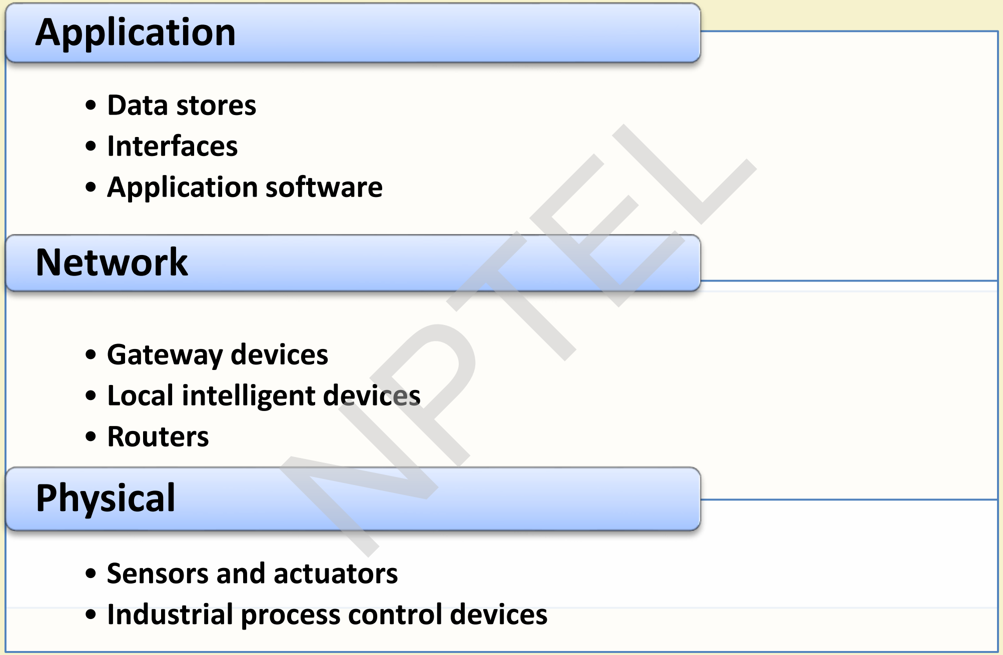
I Information disclosure

D Denial of service

E Elevation of privilege

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

# IIoT Attack Surface



**Application**

- Data stores
- Interfaces
- Application software

**Network**

- Gateway devices
- Local intelligent devices
- Routers

**Physical**

- Sensors and actuators
- Industrial process control devices

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

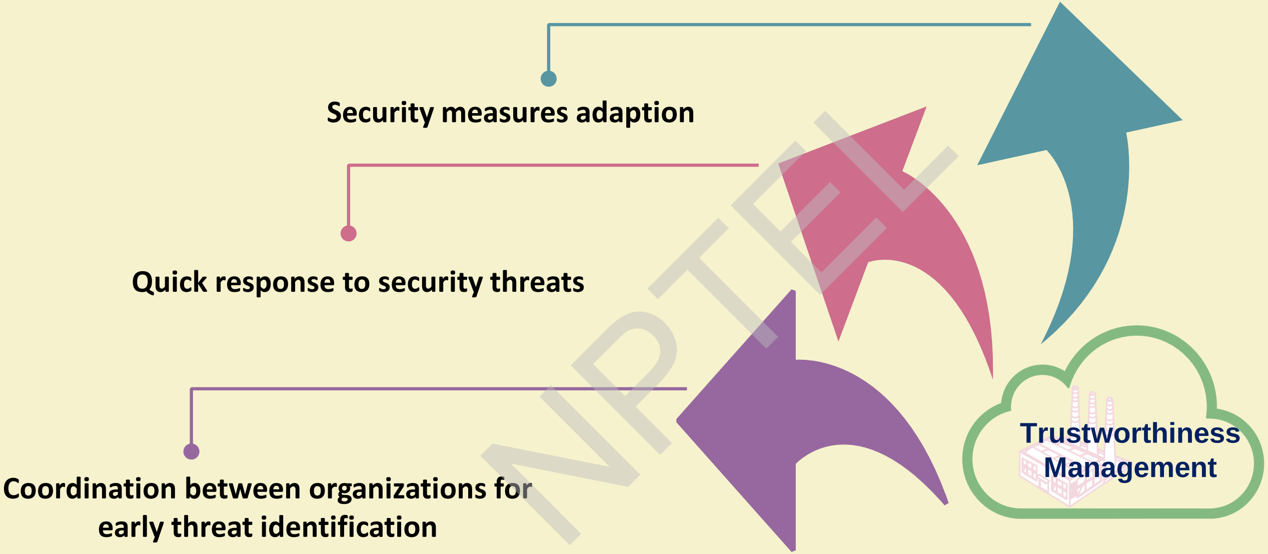
Source: IoT Attack Surface Areas", OWASP

# IIoT Attack Vectors: Physical Layer

- Impersonation attack
- Jamming attack
- Device tampering

Source: IoT Attack Surface Areas”, OWASP

# Trustworthiness Management


Security measures adaption
Quick response to security threats
Coordination between organizations for early threat identification
Trustworthiness Management

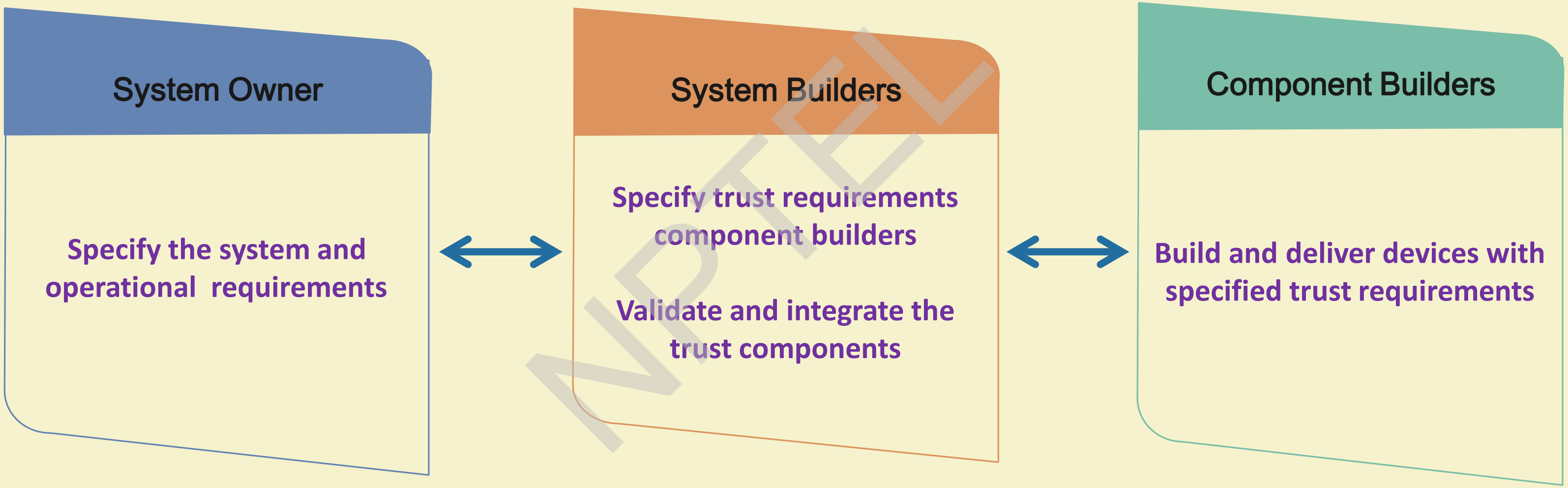
Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

# 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



System Owner

Specify the system and operational requirements

System Builders

Specify trust requirements component builders

Validate and integrate the trust components

Component Builders

Build and deliver devices with specified trust requirements

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

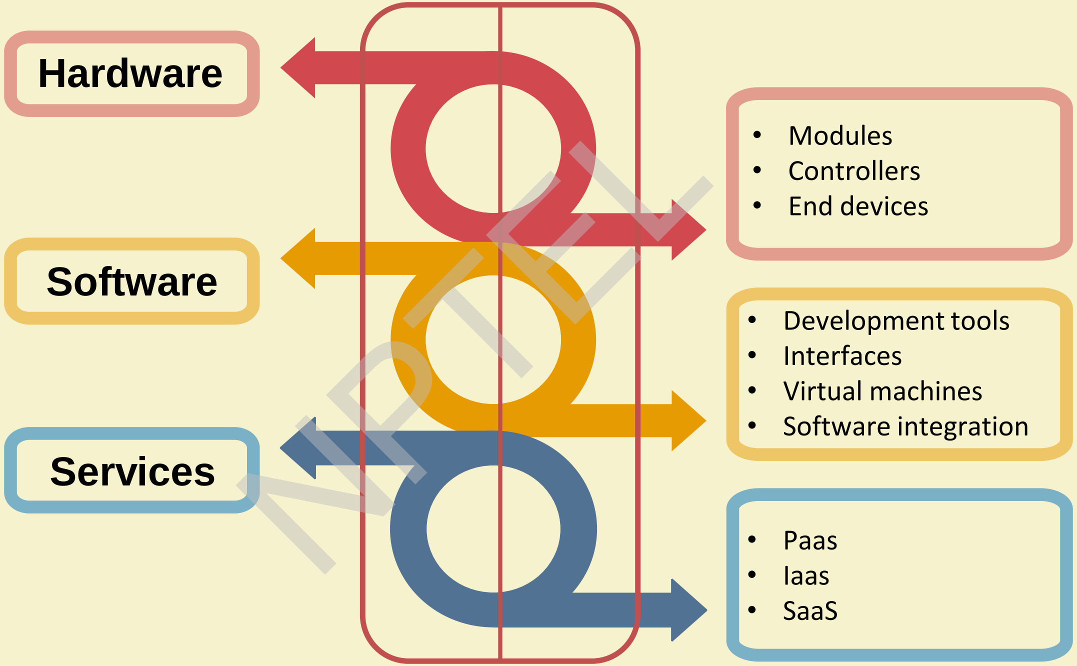
Source: "Industrial Internet of Things Volume G4: Security Framework", Industrial Internet Consortium

# 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.)



- Modules
- Controllers
- End devices

- Development tools
- Interfaces
- Virtual machines
- Software integration

- Paas
- Iaas
- SaaS

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!!