TOSHIBA

Leading Innovation

Industrial IoT Security accelerate Digital Transformation

Takashi Amano

Technology Executive
General Manager, Industrial ICT Security Center
Toshiba Digital Solutions Corporation

01 Industrial IoT Architecture

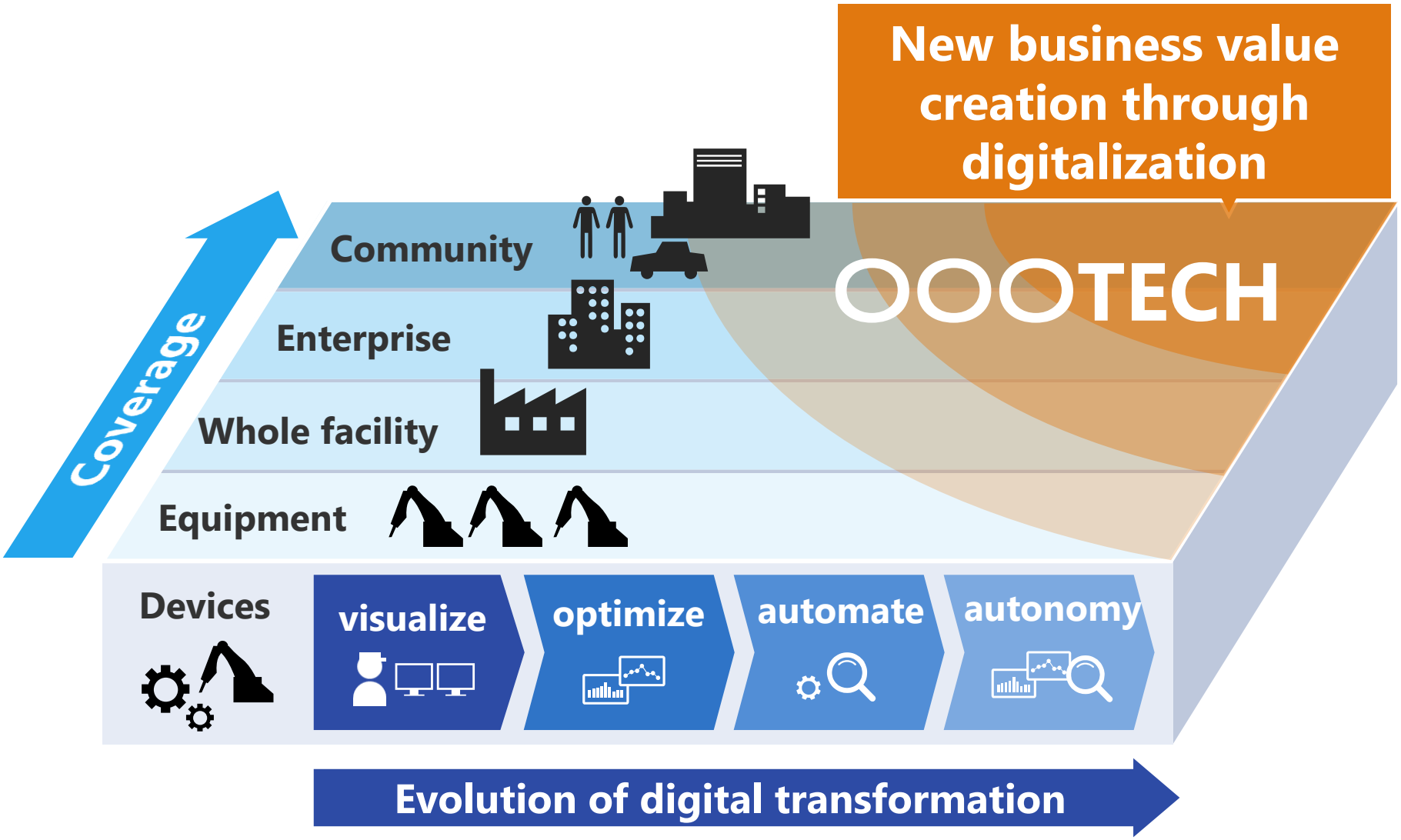
02 Industrial IoT Security

01

Industrial IoT Architecture

‘SPINEX’

Evolution of Digital Transformation



140-year Accumulated Knowledge of "Products" = Field Capability (Operation Technology)

Energy

Thermal Power Plant
Accumulated
1975 facilities

Hydroelectric Power Plant
Global share
No.1*

Geothermal Plant
Global share
No.1

Transmission & Distribution
Share in Japan
No.1

*Variable-speed pumped-storage: cumulative No. of plant installed

Social Infrastructure

Buildings/Facilities

Elevator
Share in Japan
22%

Air-conditioner
Large-scale chiller
Share in Japan
No.1

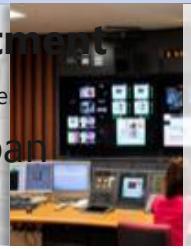
Lighting
Facility lighting
Share in Japan
20%

Building Energy
UPS*
Share in Japan
26%

*Uninterruptable Power System

Public Infrastructure

Water treatment
Monitor/electric syste
Share in Japan
No.1



Broadcasting
Share in Japan
50%

Roads
Central system
Share in Japan
No.1

Security/Automation System
OCR Letter Sorting Machine
Share in Japan
No.1

* Source: Toshiba research.

Improving Manufacturing Process by AI
（Toshiba Semiconductor Fab）

Manufacturing Process

Rate of defect classification 49% ➡ **83%**

50 models **20,000 process**

Time to identify problem causes 6hrs ➡ **2hrs**

Production Equipment

2016 The Japanese Society of Artificial Intelligence **200 types** **4,000 machines**

Field Innovation Award **Gold**

Processes 2bil. data sets per day through AI

Utilizing IoT Data Generated from Toshiba Office Facility (Lazona Kawasaki Toshiba Building)

BEMS for total optimization

Operation Start Time

November 2013

achievement

35.2%

CO_2 Reduction

FY2016

54.0%

For whole building

Number of sensors

35,000 sensors

Energy Conservation Grand Prize

Chairman Prize of ECCJ*

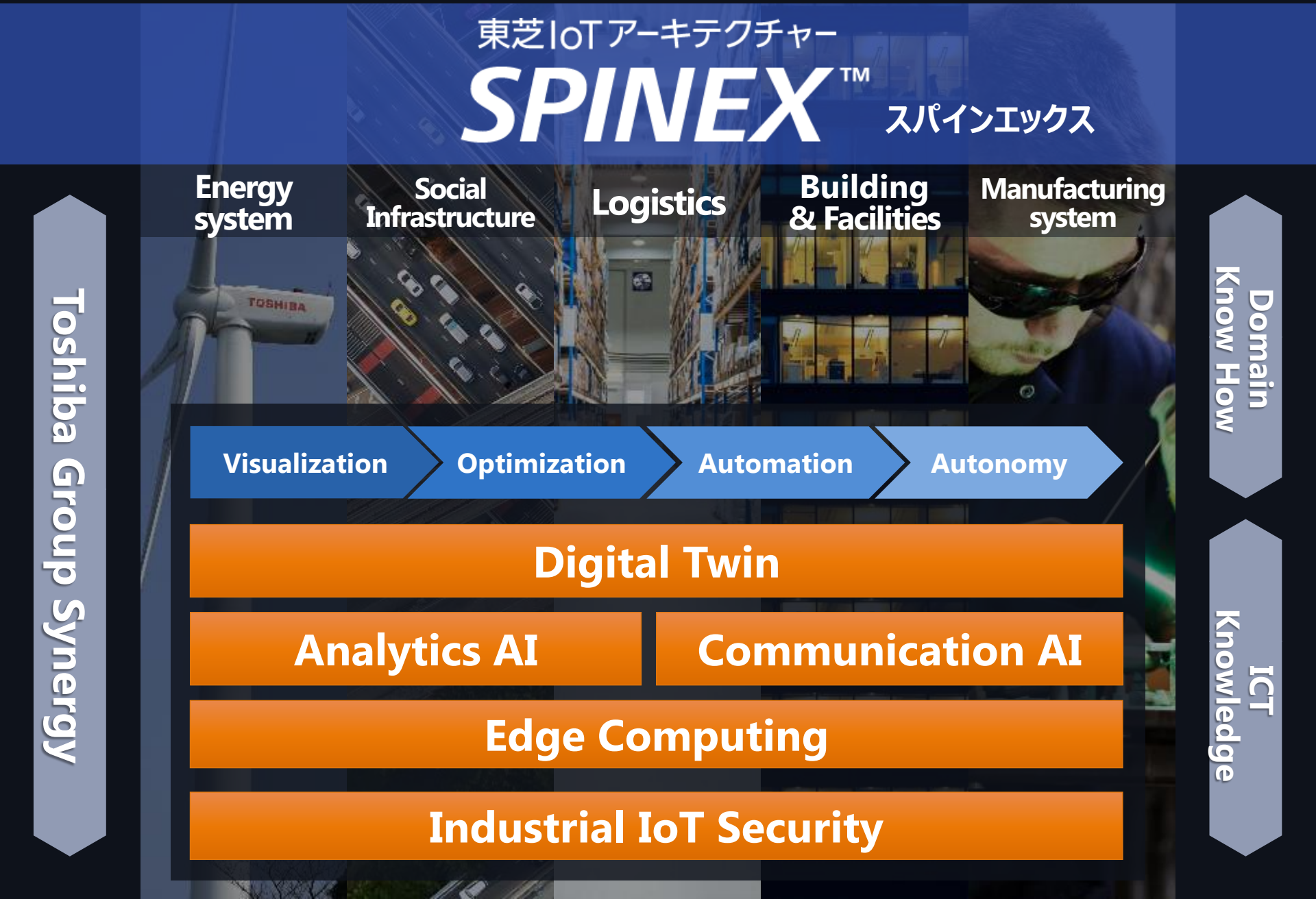
Awarded

*ECCJ: Energy Conservation Center, Japan

30Bil. RAIords

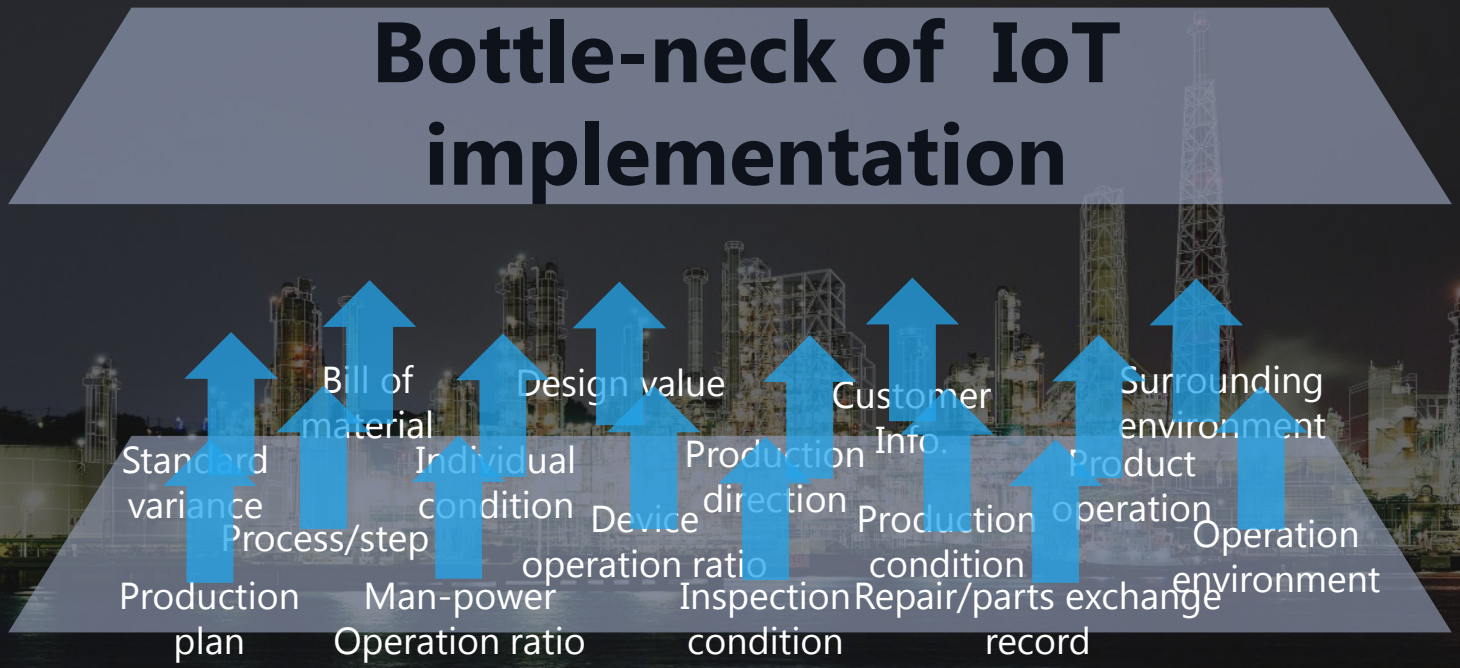
Collected data + analysis of data

Toshiba IoT Architecture



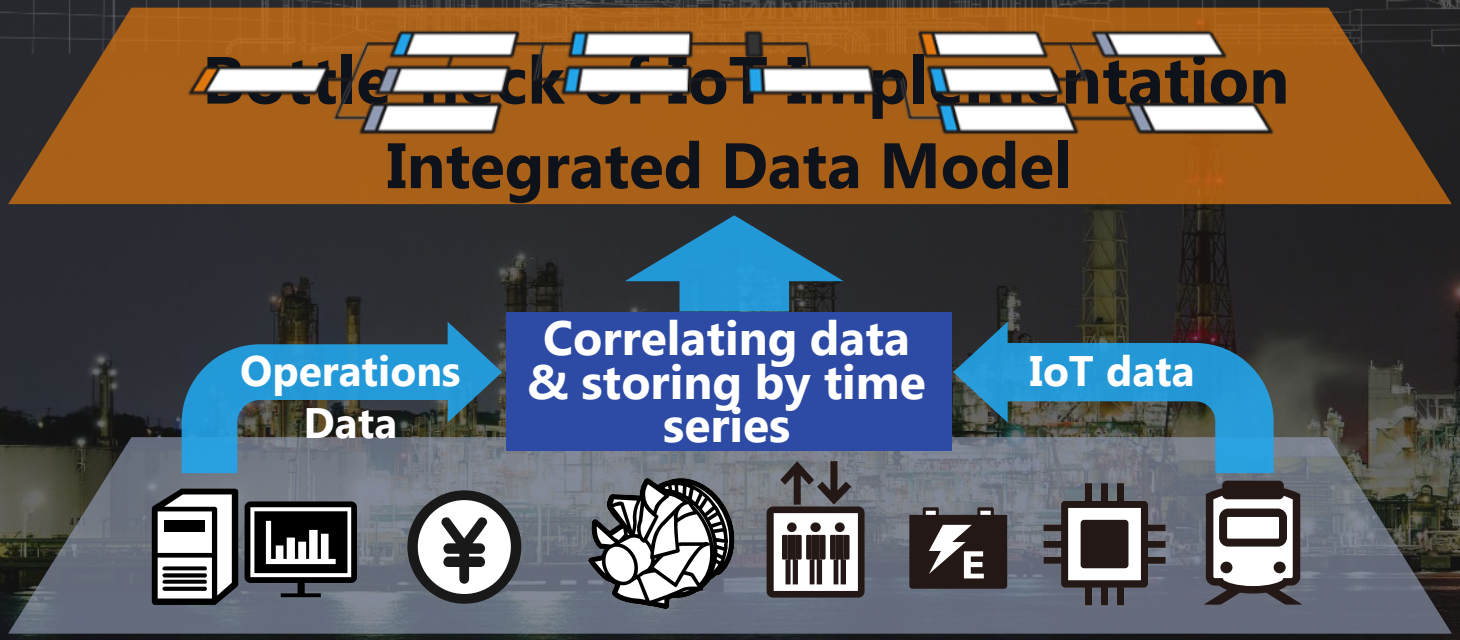
SPINEX_digital twin

Sensor data generated need to be structuralized before utilization.

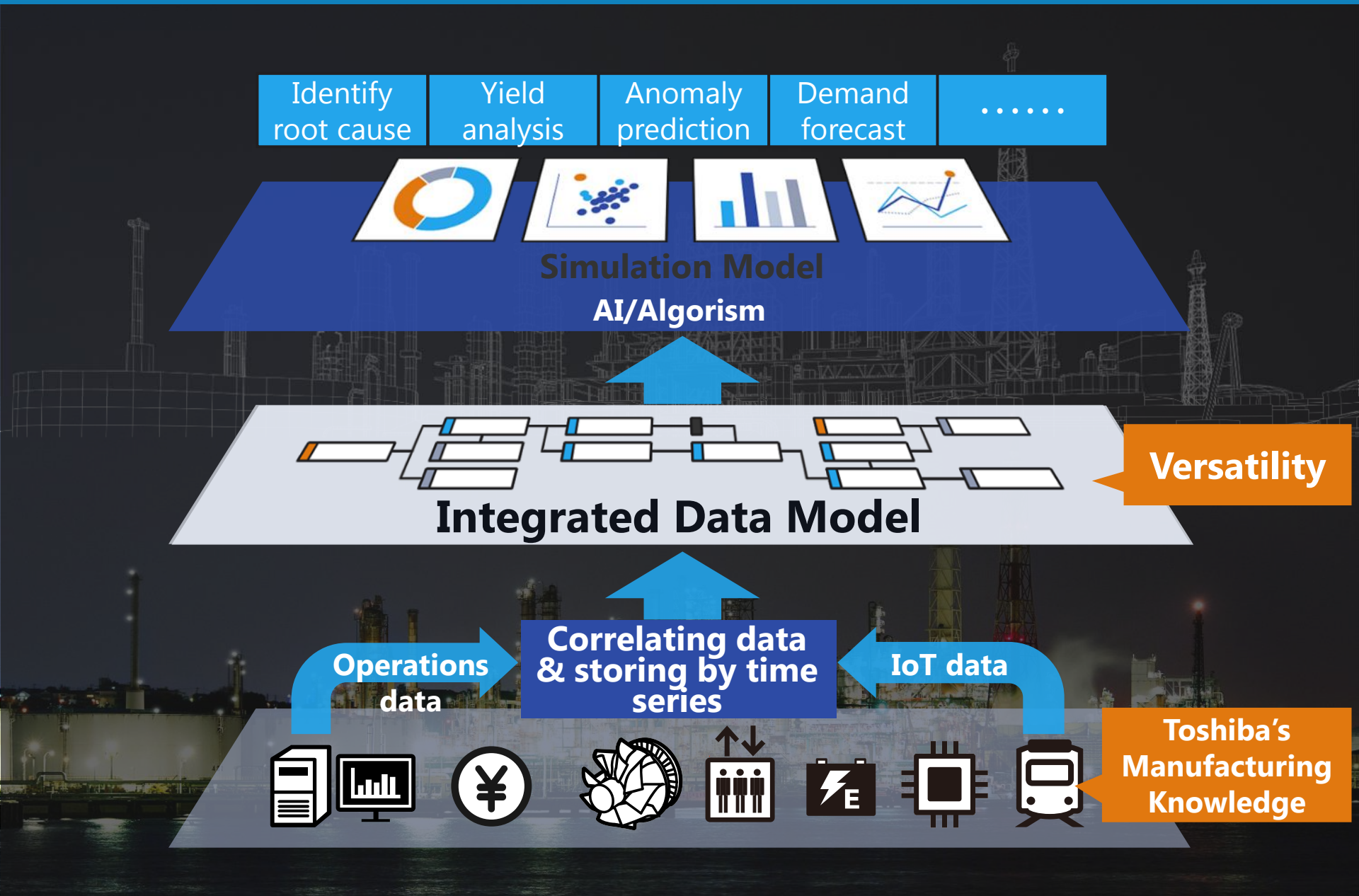


SPINEX_digital twin

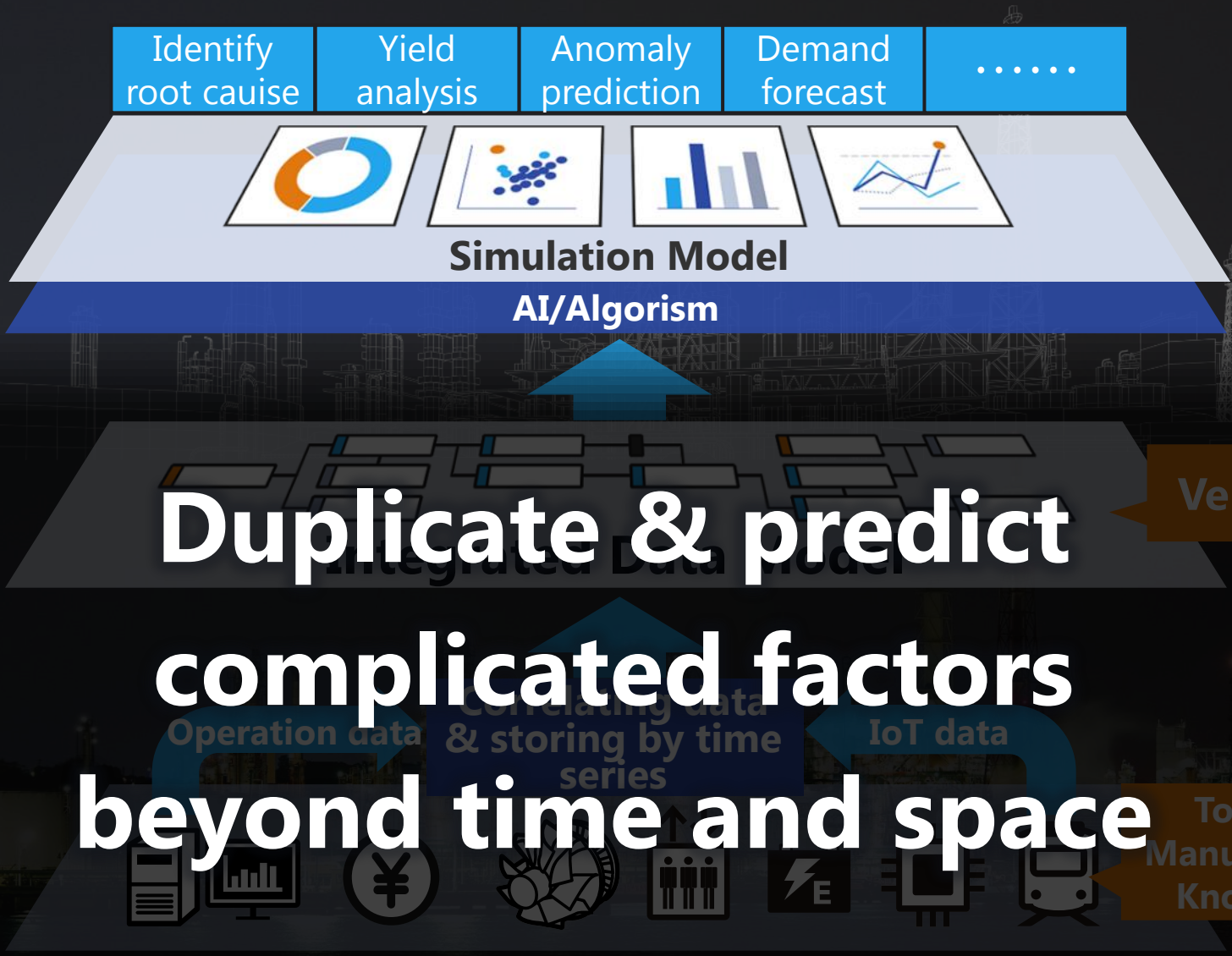
IoT implementation time can be dramatically reduced by using an integrated data model correlating IoT data and operations data.



SPINEX_digital twin



SPINEX_digital twin



Duplicate & predict complicated factors beyond time and space

SPINEX_ai service

Toshiba IoT Architecture

SPINEX™

SATLYS™

Solutions by AI Technologies for anaLYSis

AI for things

RECAIUS™

REConize with AI + us（people）

AI for humans

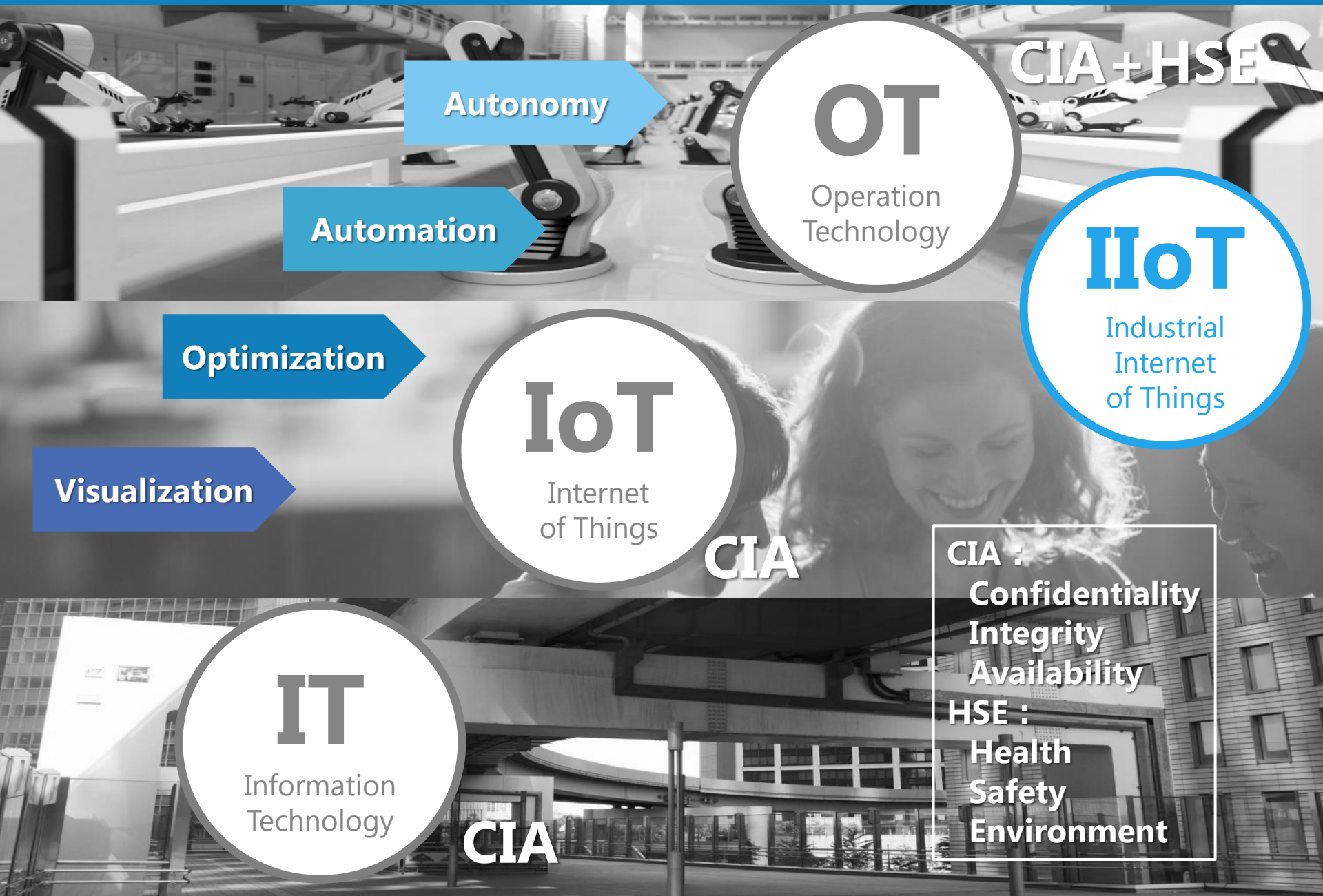
Announced on 30/10/2017

Being Connected : Philosophy of SPINEX™

02

Industrial IoT Security

Industrial IoT Security



Security in Digital Transformation era

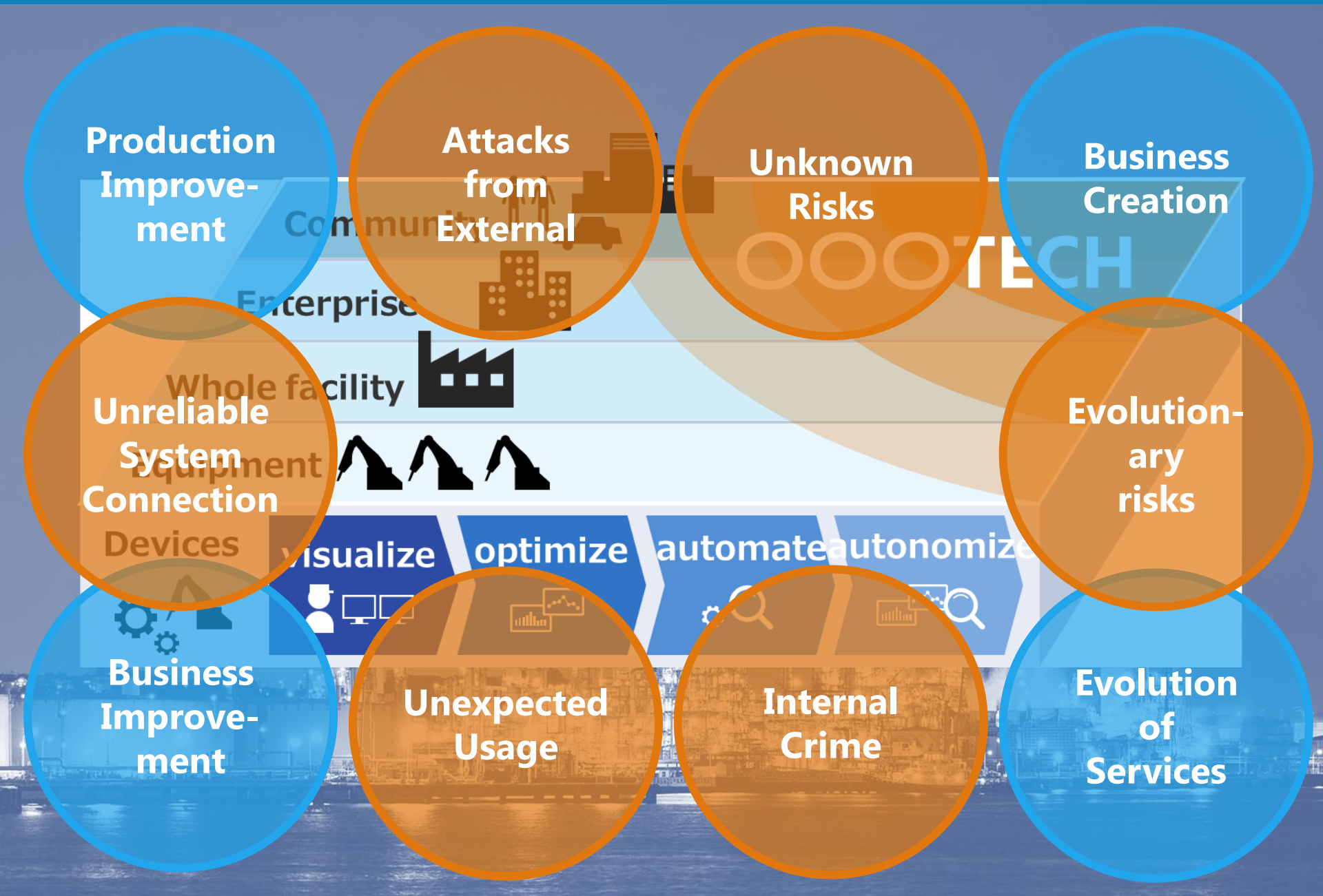
Every Things and Systems connect to the network

Treats of cyber attack expand from information leakage to physical damage

▼

Sustainable security is needed for social infrastructure and control system

Values and Threats in Digital Transformation



What to protect at Industrial IoT

People

Health, Safety, Environment

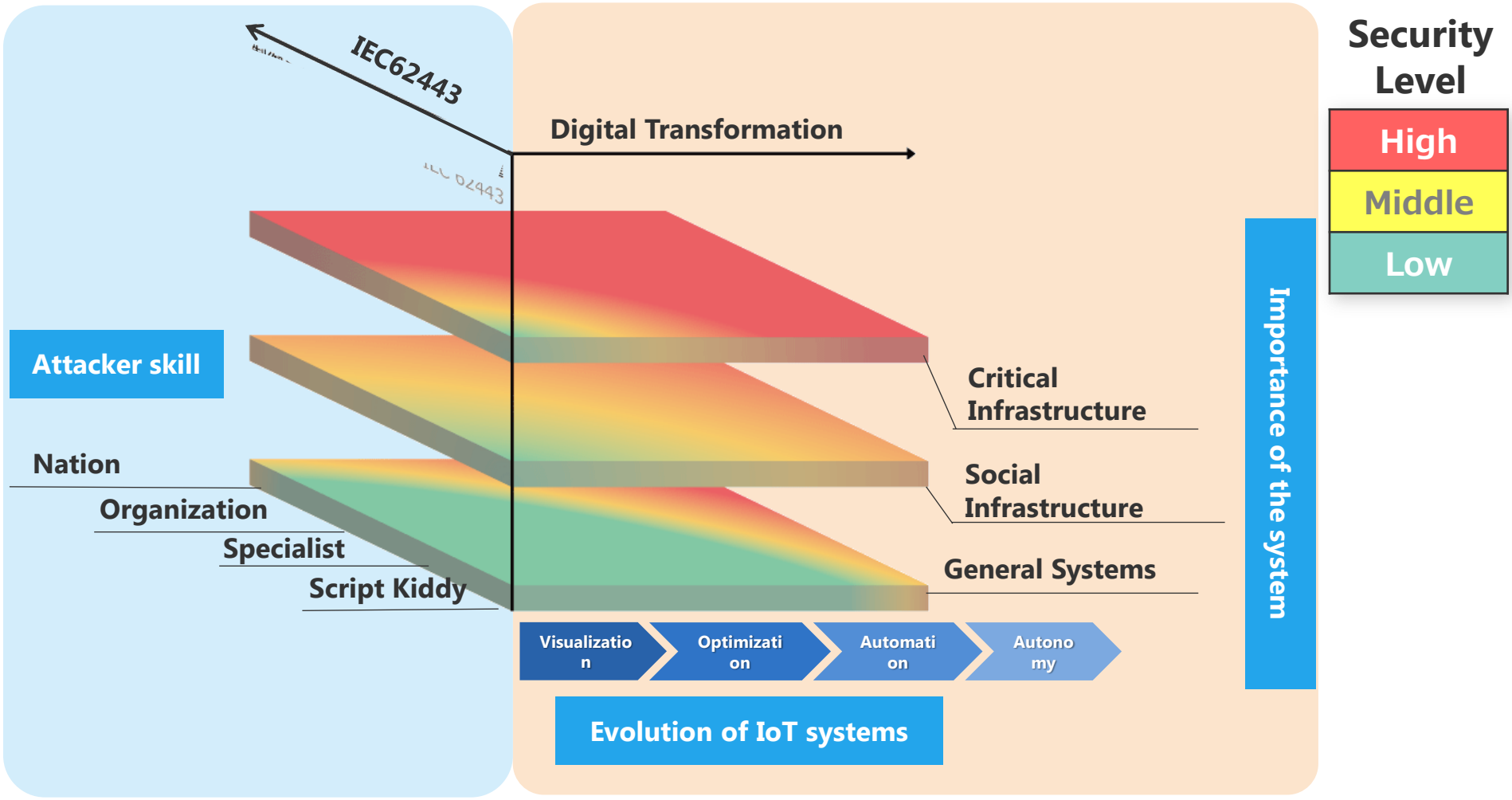
Things

Normal operation of devices and systems,
Early detection and restoration of cyber attacks

Data

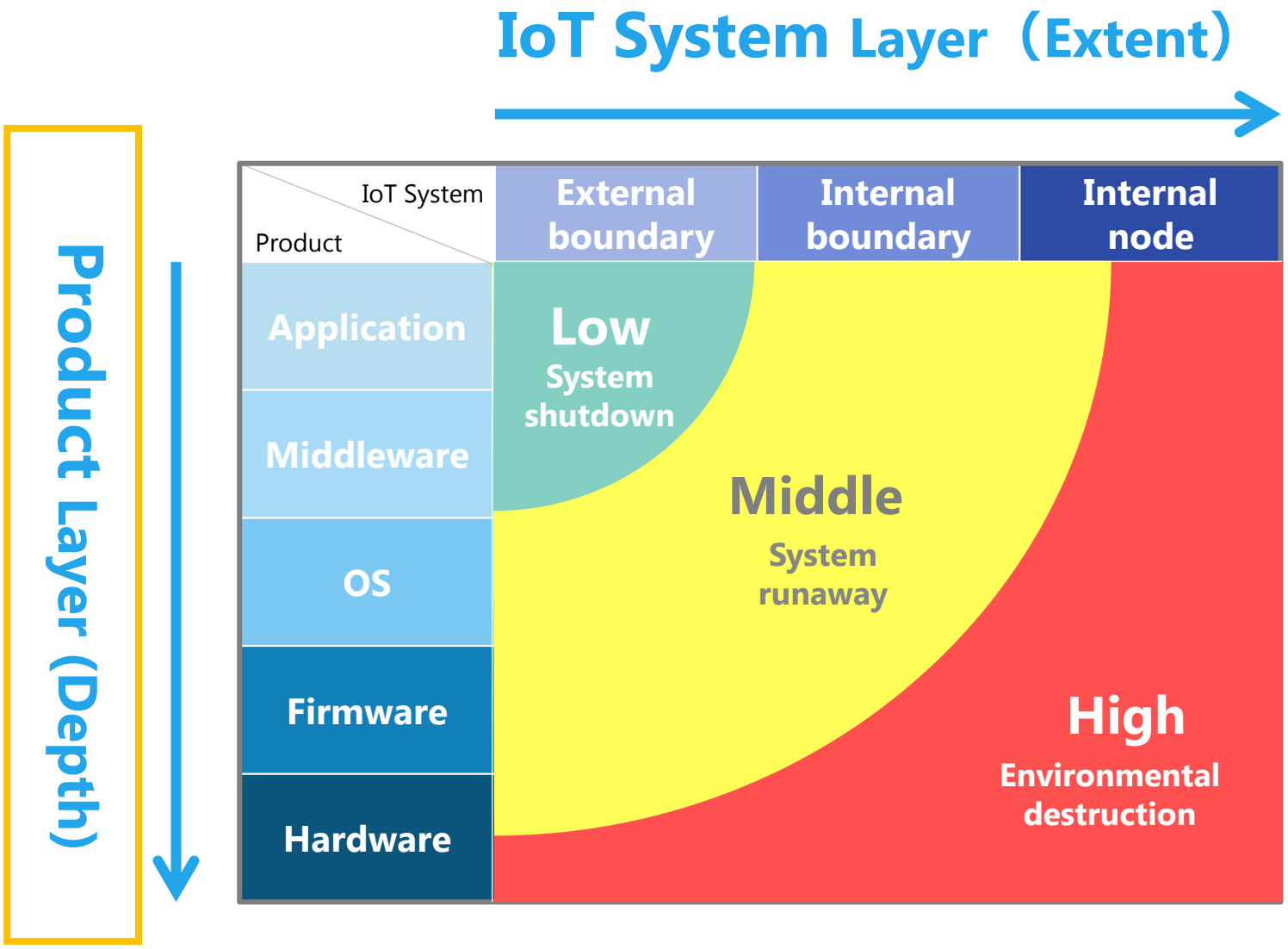
Manufacturing know-how, craftsmanship, production data, recipe, ...

TOSHIBA Industrial IoT Security Reference Architecture

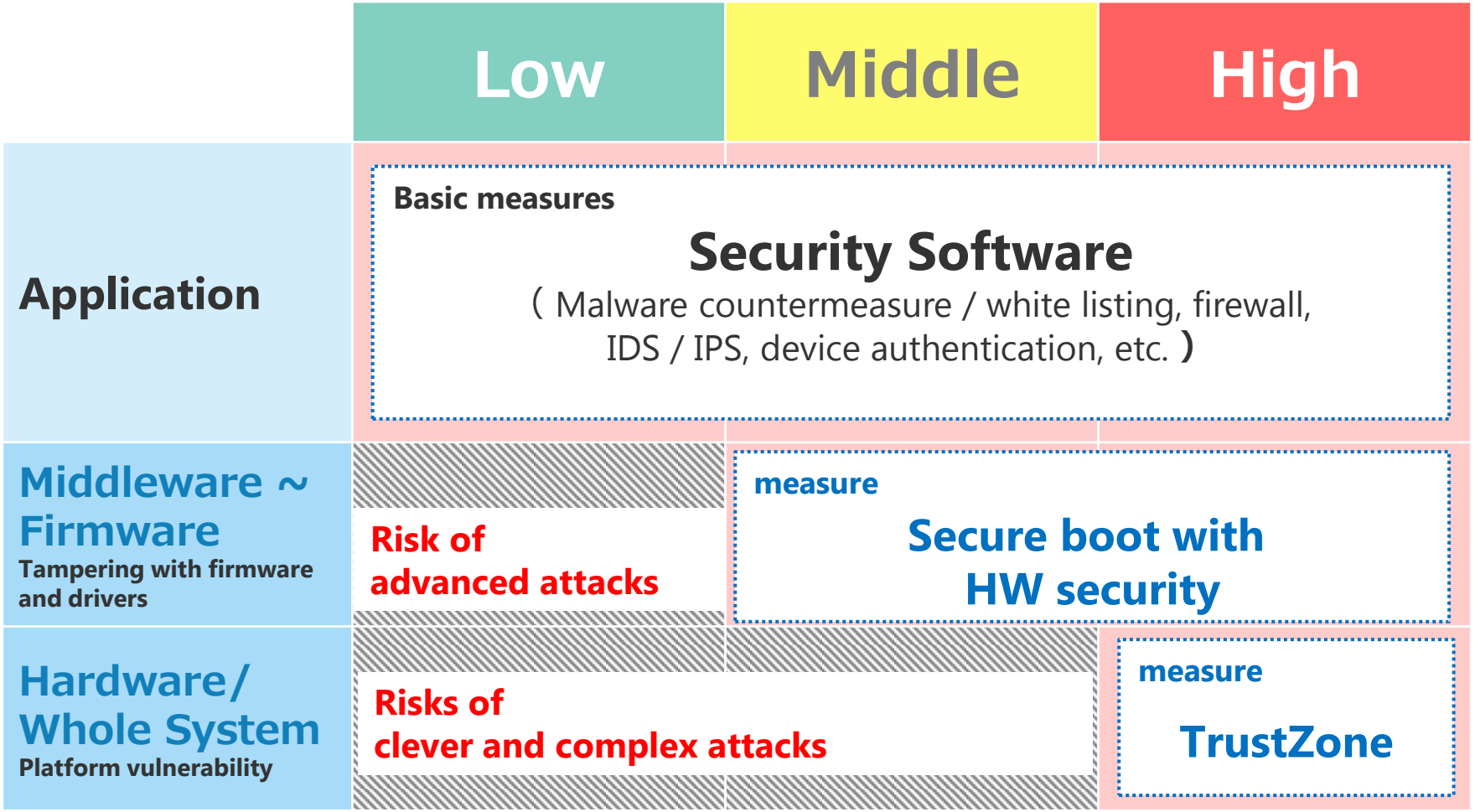


Depend on the progress and importance of the system Required and sufficient security measures considering cost balance

Multi-layer defense “Extent” and “Depth”

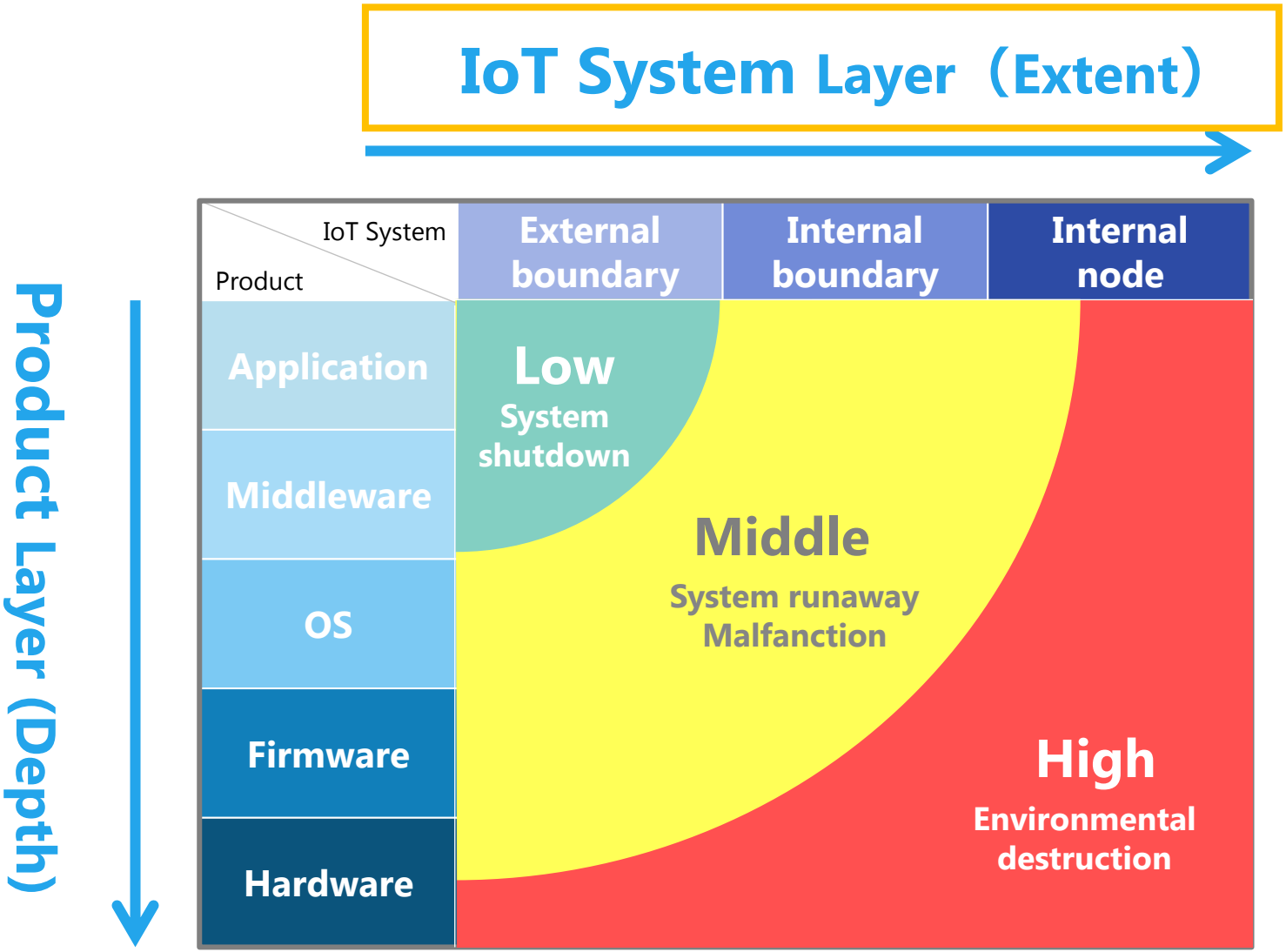


Multi-layer defense “Product Layer”



Protection against edge device threats

Multi-layer defense “Extent” and “Depth”



Multi-layer defense “IoT System Layer”

External boundary	Internal boundary	Internal node

Visualization → Optimization → Automation → Autonomy

①Out-Of-Bound

Separate OT and IoT

Data integrity

②TOUCH

External connection point of OT, limited function

Device authentication

White list type command execution

③INLINE

Control system security measures

Functional safety

Malware Intrusion detection

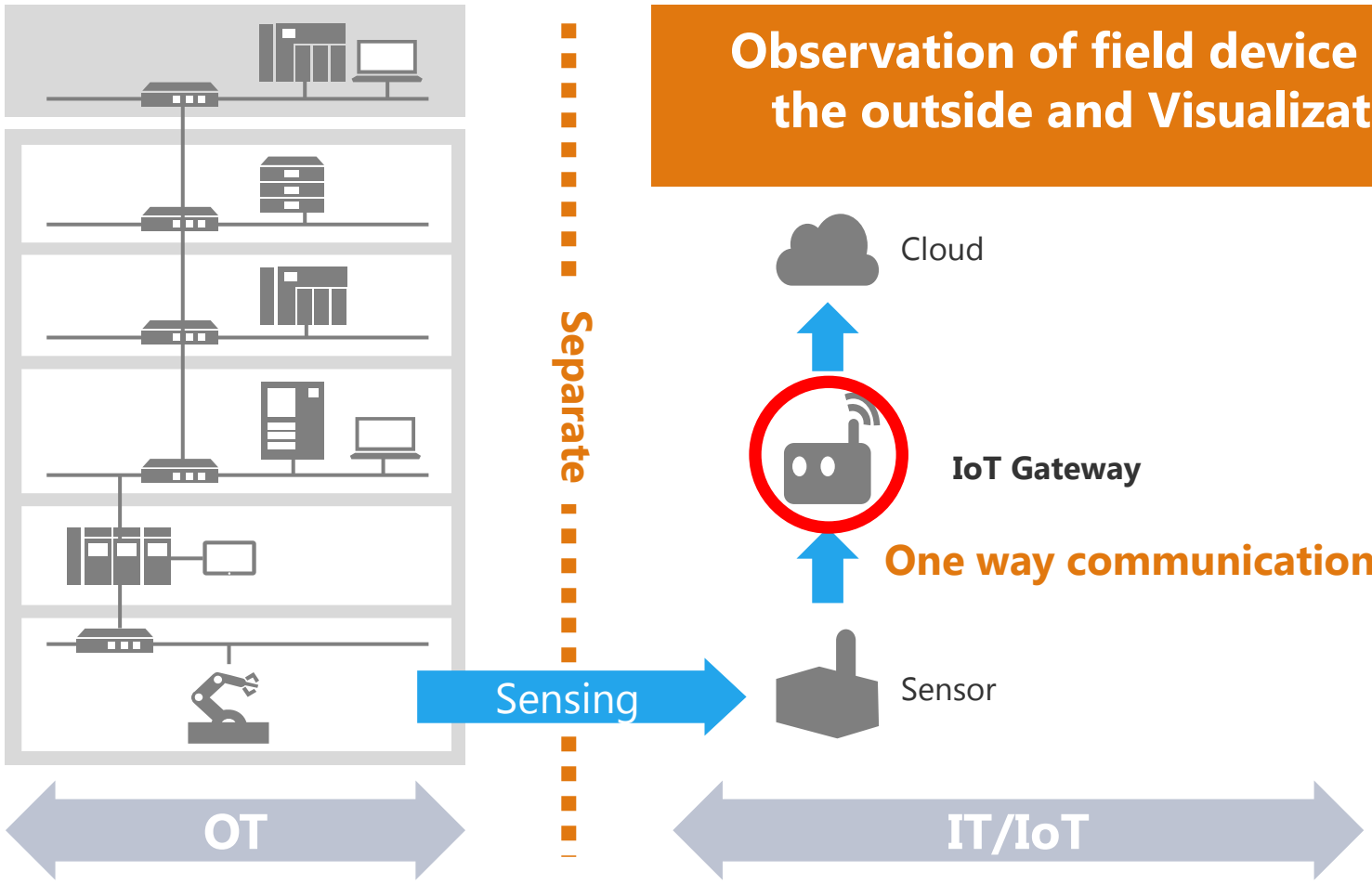
Device hardening

Physical security

The security model changes as IoT system Layer evolves

①OOB(Out-Of-Bound) Model

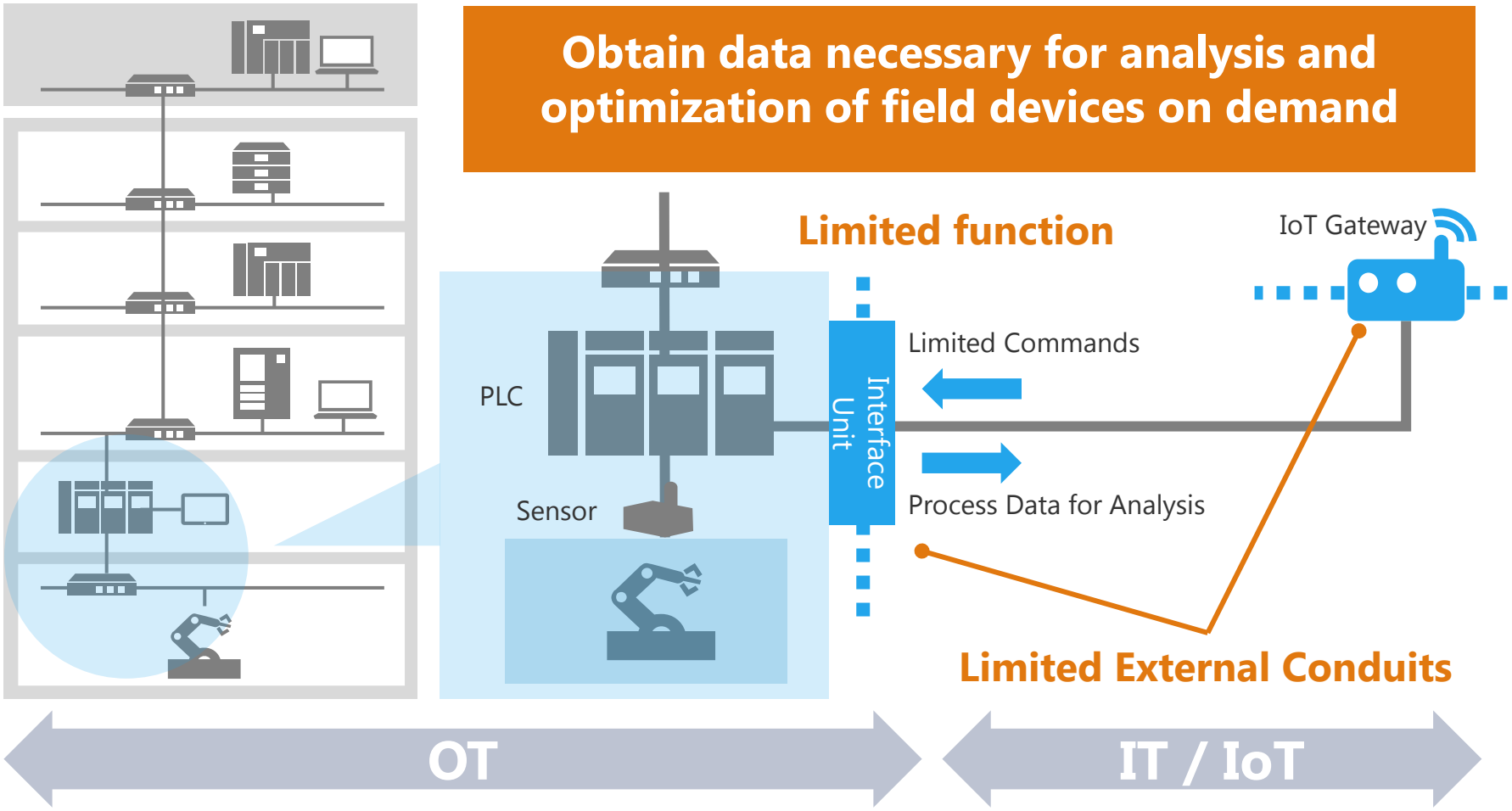
Visualization | Optimization | Automation | Autonomy



Separate OT and IoT
It does not directly affect the control process

②TOUCH Model

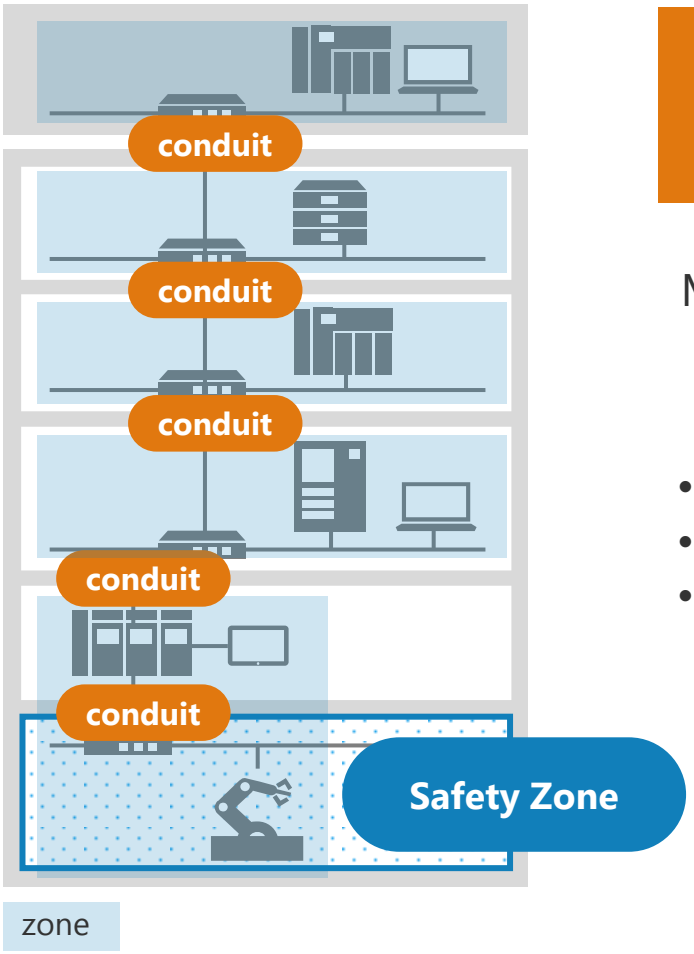
Visualization | Optimization | Automation | Autonomy



Limited external connections and functions
It does not affect important functions of the control process

③INLINE Model

Visualization | Optimization | Automation | Autonomy



Automatic and autonomy operation of control system

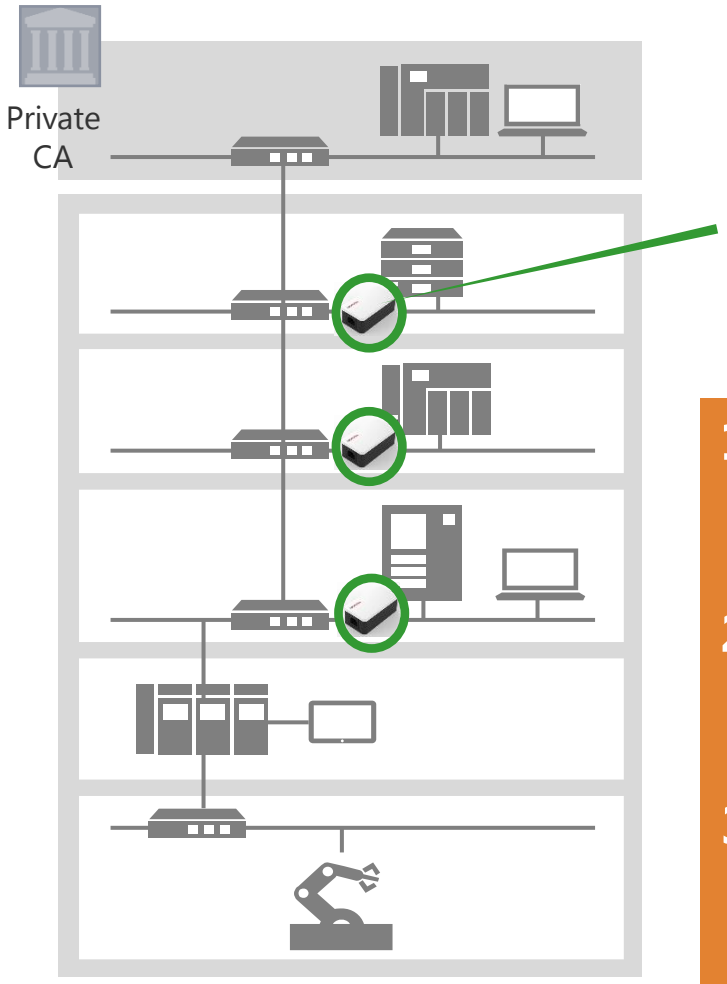
Measures compliant with control system regulation

- Zoning inside the system as functional unit
- Understand conduits between zones
- For zones close to the field,
  measures against HW level

Safety & Security

Define system zone, Localize the damage by measures of conduits exceeding the zone

Measures for legacy devices (A case of INLINE Security)



Secure security without changing existing system by inserting
Secure Proxy Device just before endpoint legacy device

1. **Protect endpoints from malware / ransomware**
2. **Secure endpoint communication (mutual authentication between devices)**
3. **Secure endpoints on behalf of security functions such as key management and signature verification**

Security enhancement for legacy endpoint is required

Life Time Protection for Social Infrastructure

Monitoring

Security Operation Center

Cooperation with internal and external companies
Detect threats from both cyber and real

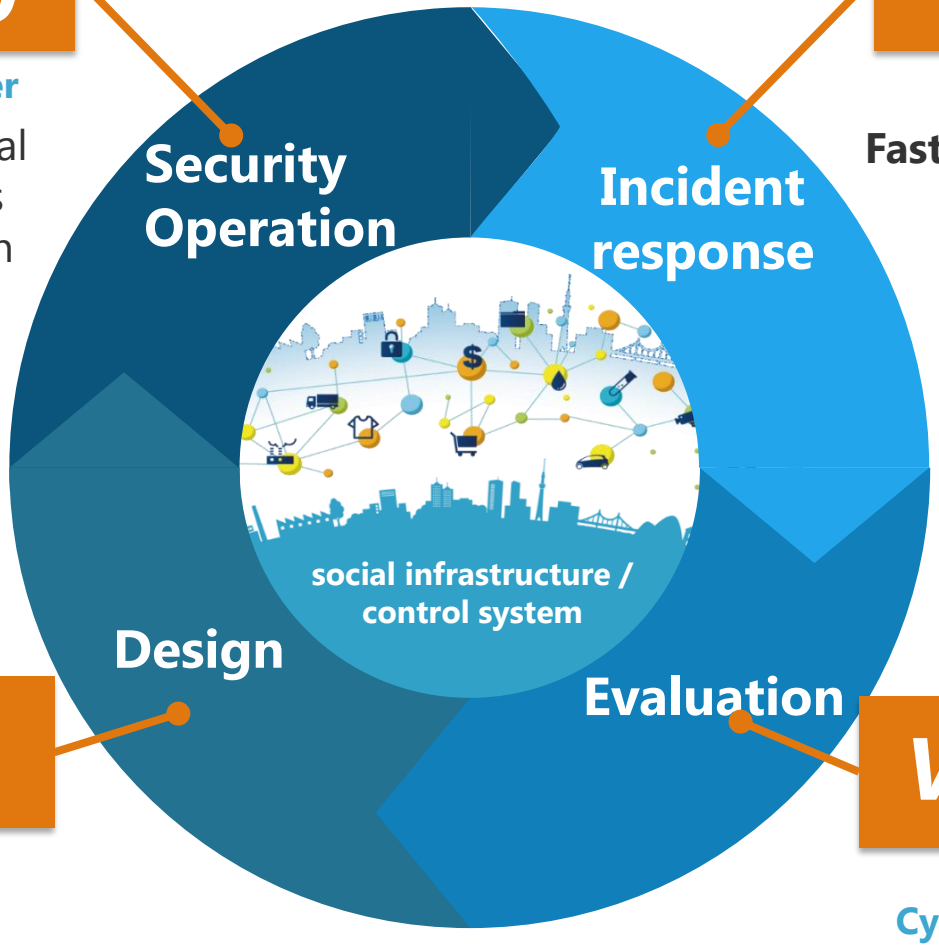
Knowledge of Real world system and things

Readiness

CSIRT/PSIRT

Fast adaptation to unknown attacks and incidents

Knowledge of cyber world attacks and threats



Defense

Security Assessment
Security by Design

Multi-layer defense in two axes according to the evolution and importance of the system

Verification

Penetration test
Cyber security exercise

Adaptive evaluation and verification for future threats


TOSHIBA
Leading Innovation