# Public-private collaboration and RRI (Robot Revolution Initiative) for Connected Industries

Nov. 30, 2017 Hideaki Omiya Chair Robot Revolution Initiative



#### **Contents**

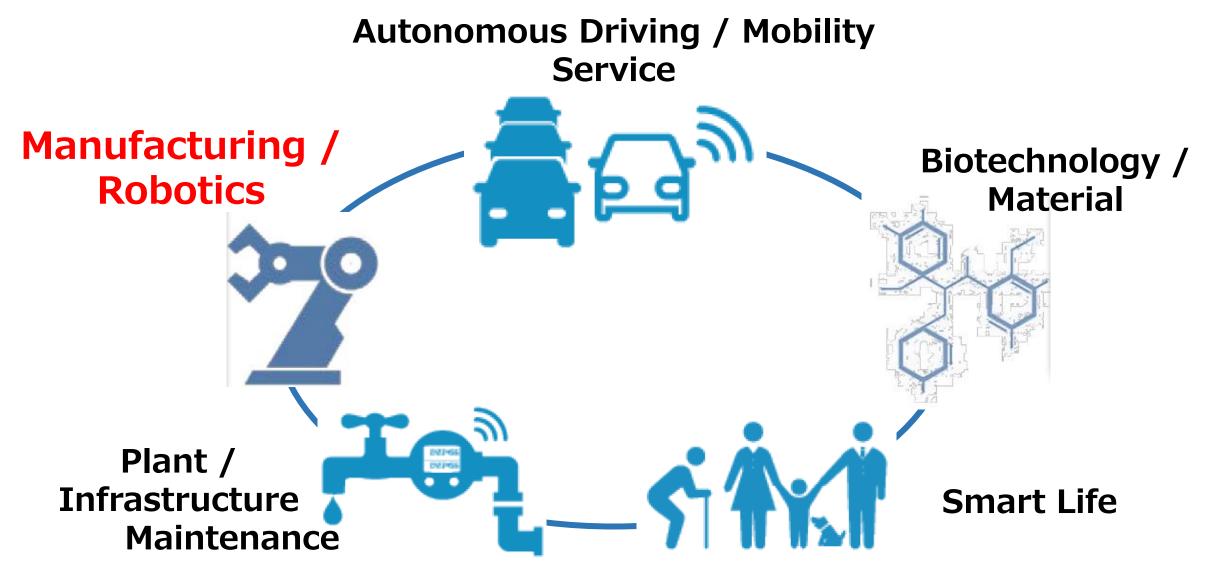
"Connected Industries"

New vision for the future of Japanese industries

- 1. Role of RRI in Connected Industries
- 2. Activities of RRI
  - 2.1 Basic Policy of RRI
  - 2.2 International Collaborations
    - 1) International Collaborations Overview
    - 2) Major Standardization Activities
    - 3) IEC (International Electrotechnical Commission) activities in Japan
    - 4) Industrial Security (Hypothesis of IIR)
  - 2.4 Building of Nationwide Network
  - 2.5 Collaborations with Related Organizations
- 3. Still hesitating to connect?
- 4. Expectation to today's Symposium

#### **Role of RRI in Connected Industries**

"Connected Industries"



Source: METI

## **Basic Policy of RRI**

-- We, the private sectors should consider to change our manufacturing business

-- Japan has rich and high quality real-side data

Can contribute to the world in a unique way

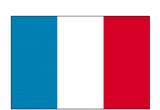
#### **International Collaborations Overview**

"Connected Industries"

## with Europe













with U.S.



## **International Symposia**













Exhibitions





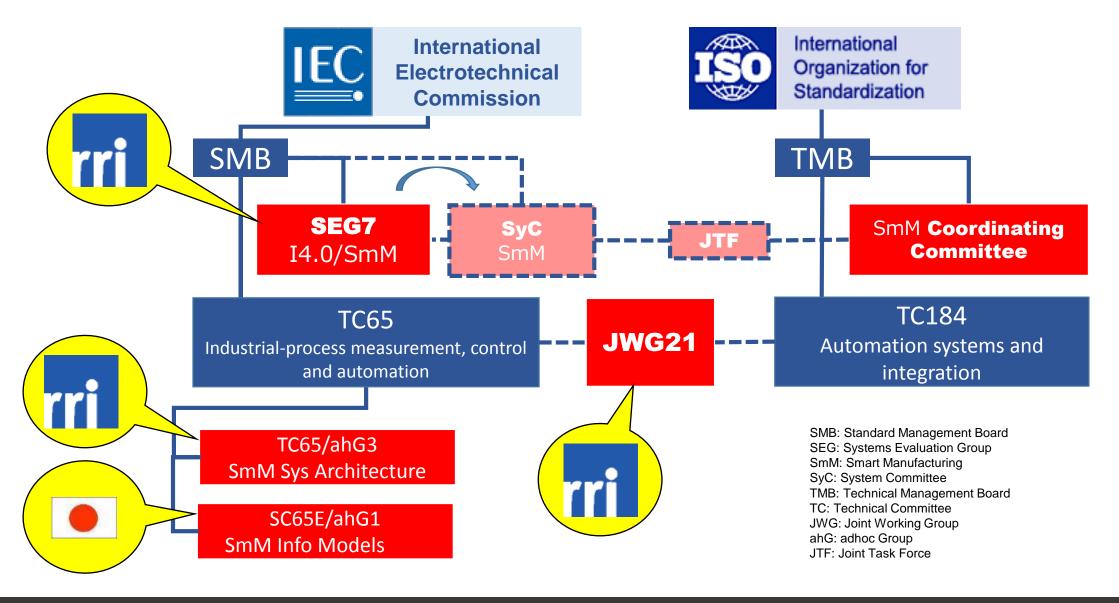




## **Major Standardization Activities**

#### "Connected Industries"

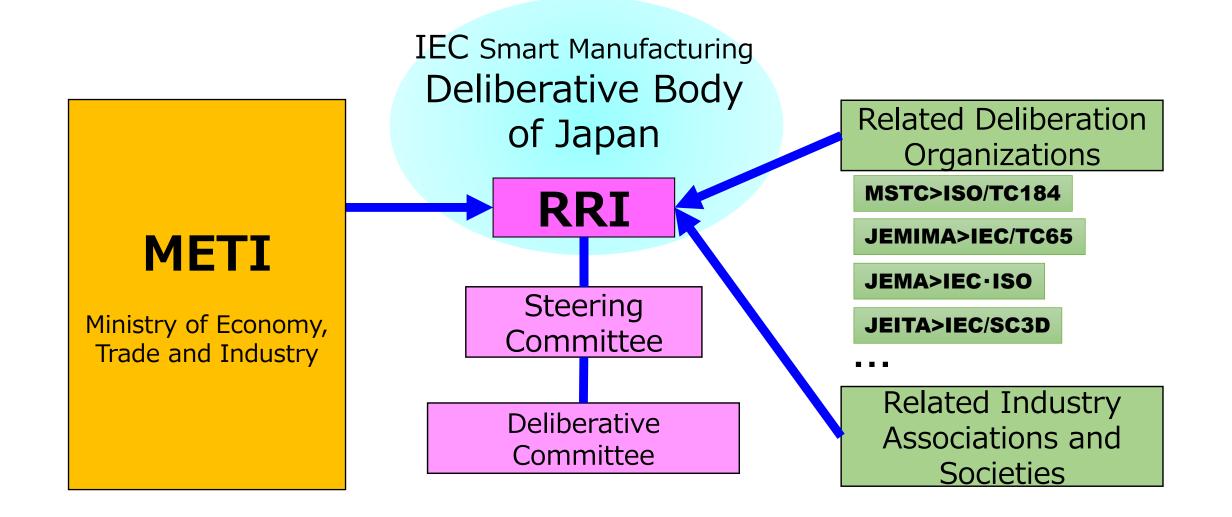
New vision for the future of Japanese industries





#### IEC Smart Manufacturing activities in Japan

New vision for the future of Japanese inc



## **Building of Nationwide Network**

#### "Connected Industries"

New vision for the future of Japanese industries









## Collaborations with Related Organizations onnected Industries vision for the future of Japanese industries

- Industry Associations
  - Electric
  - Machine
  - Information
  - Electronics
  - User / Operation Technology
- Learned Societies
- SME Supporting
- Cross-cutting / Other related organizations

### **Industrial Security** (Hypothesis of IIR)

- It is impossible to avoid cyber attacks if legacy devices are included
  - Invaded by unknown thread -> 97% of enterprises
  - Average days to detect invasion -> 205
  - Malware that cannot be detected by anti-virus software -> 55%
- Need to consider quick recovery after attack detection
- Consideration in following fields are necessary
  - Legal (including data usage)
  - Enterprise / Organization
  - Supervisory system (including self/third party certification, etc.)
  - Standardization
  - Technology

# Still hesitating to connect?

### **Our Background**

- "Connecting with other companies" is not yet very easily accepted
  - -- Experience that companies have gained by competing with many other companies for long time
  - -- Experience that companies have gained by not connecting and differentiating from other companies

Need to understand that the current situation does not allow us to deny the "value of connecting" any longer

## **Expectation to Today's Symposium**

"Connected Industries"

New vision for the future of Japanese industries









#### ロボット革命イニシアティブ協議会

**Robot Revolution Initiative** 



Future image of Manufacturing and Service with IIoT

Harmonizing Smart
Manufacturing
Standards with
usecases

Extracting Industrial Security Issues with usecases