Industrial IoT Networking – Reshaping The Factory

PC Lee

Renesas Electronics Taiwan
Agenda

- The Next Industrial Revolution
- Components of the Industrial IoT Network
- New business models and opportunities
- Summary
Industrial IoT Is Changing The Typical Definition

Mobile Device Are The Center of IoT

Vertically Oriented Machine 2 Machine

Process & Cyber Physical Systems Are The Center

Secure, Global, Real-time Access to Data and Analytics
Industrial IoT: Next Industrial Revolution

1st Industrial Revolution

- Powered loom ca. 1845
- Machines with mechanical gears, powered by water and steam

2nd Industrial Revolution

- Ford Model-T ca. 1927
- Assembly line for mass production, common parts, process efficiency

3rd Industrial Revolution

- Honeywell controls ca. 1970
- Invention of the semiconductor, programmable systems
- Electronic and IT systems to automate production; IE
- Internet and networking integration

4th Industrial Revolution

- Trending

© 2015 Renesas Electronics Corporation. All rights reserved.
Imagining The Industrial IoT – Airlines

Dispatching service persons before arrival

Analyzing real-time performance data

Bringing in the right service part

10% Of Flight Delays from unscheduled maintenance issues

$8B In Additional Costs

© 2015 Renesas Electronics Corporation. All rights reserved.
Imagining The Industrial IoT – Factory

**Sensor-Enabled Automation**
Sensors throughout factory assets and operators to prevent unplanned downtime and boost productivity

**Virtual Manufacturing**
Using digital and collaborative tools to model plants, operations, product development

**Real-time Analytics**
Data driven analytics to optimize throughput and reduce waste

**Cyber Physical Systems**
Agile production cells and operations between human and robot-supported work for efficiency and customization

**IIoT Economic Impact To Manufacturing Estimated at $1.2 Trillion**

Sources: IIC, Accenture, GE
IIoT Is Mobilizing The Industry

Machinery Manufacturers Need IIoT

Traditional

Future

Product Transaction Model
Customer Relationship Model

“Gartner estimates IoT suppliers will generate incremental product and service revenue exceeding $300B by 2020”

Lesson: Find Strategic Partners!
Industrial OEMs Creating New Revenue Streams

- Site dashboard
- Customizable metrics
- Track performance
- Sustainability tools
Challenges Related to Widespread Adoption

No definitive technology and approach
  - Industry 4.0 vs. IIoT vs. M2M
  - Consortia race

Interoperability & Standards
  - Data structures that are proprietary
  - Industrial Ethernet is very fragmented

Business justification
  - Cost of retrofitting into existing infrastructure
  - Management of large-scale collection and correlation of data
  - Perceived and real security risk

Expertise gaps
  - Lack of expertise focused on the ‘digital workplace’
  - Differing fields and domain expertise – IT vs. OT gap

Source: Industrial Internet Consortia
Main Components of Industrial IoT Solutions

Seamless Operation of People, Assets, & Process
- Technology-enhanced with sensors, feedback mechanisms
- Autonomous to the point of ‘self-aware’
- Configurable, customizable

Connected
- Real time, non-real time domains
- Wired and Cloud components

Safe & Secure
- Inherent safety
- User authenticated, context aware security

Intelligent Analytics
- Descriptive, Predictive and Prescriptive Analytics
- Conditioned at each plant level

Managed Data
- Reusable, scalable data models
- “Intelligent Information” when and where people are
Industrial IoT Operations at Each Level

Enterprise Level

Control Level

Field Level

IIoT Opportunities Start At The Edge
Volkswagen German Plant Accident: Robot Grabs, Crushes Man To Death
Safety Is Priority #1

Productivity and Safety go hand-in-hand

- OSHA estimates lost productivity of $60B/year

Costs of non-compliance

- Violations/fines, higher insurance premiums, workers compensation, litigation, etc.
- Machinery Directive (IEC 61508) requirement in EU

Market differentiator

- Safety certified products and systems give ‘quality’ confidence

Challenge: Cost Burden and Lack of Expertise
Certified Safety Solution Reduces Time And Risks

Developed according to IEC61508:2010
  - Targeting SIL2 and SIL3 applications

Multiple platform solution
  - RX631/RX63N and RX111

Comprehensive Solution
  - Self-Test Diagnostic Software
  - Comprehensive Safety Manual including Test Plan & Analysis, FIT data, etc.
  - Developed with FS certified IAR Systems Embedded Workbench for RX (EWRXFS)
  - Scalable to other RX platforms

Cuts Safety Certification Process by 6 Months!!
Comprehensive Fault Coverage Validation

• Diagnostic coverage of CPU validated by fault injection using real hardware netlist of the MCU

• Evaluated the coverage of each injected fault (detected or not detected)

• Over 39 Test Segments and full set of CPU instruction set

• Exhaustive fault injection tests with >190,000 possible faults (ex. RX631/63N)

• Diagnostic Coverage (DC) value reaches >90%
# Microcontroller Element Analysis

## Relevant MCU elements covered

<table>
<thead>
<tr>
<th>MCU Element</th>
<th>Element Description</th>
<th>ElementFIT for failure mode 'permanent'</th>
<th>ElementFIT for failure mode 'transient'</th>
<th>Diagnosis &amp; measure (DH-ID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O (chip I/O &amp; Controller)</td>
<td>Chip I/O logic</td>
<td>0.425</td>
<td>1.124</td>
<td></td>
</tr>
<tr>
<td>UART modules, one channel</td>
<td>UART communication interface</td>
<td>0.229</td>
<td>1.472</td>
<td></td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td>Temperature sensor circuit</td>
<td>0.150</td>
<td>0.024</td>
<td></td>
</tr>
<tr>
<td>MCK_TPU</td>
<td>Frequency measurement circuit, can be used to monitor the main clock, sub-clock, LOCO, PLL and HOGO for abnormal frequencies; clock count extension circuit of TPU</td>
<td>0.001</td>
<td>0.002</td>
<td>used for diagnosis</td>
</tr>
<tr>
<td>MCK_MTU2</td>
<td>Frequency measurement circuit, can be used to monitor the main clock, sub-clock, LOCO, PLL and HOGO for abnormal frequencies; clock count extension circuit of MTU2</td>
<td>0.001</td>
<td>0.002</td>
<td>used for diagnosis</td>
</tr>
<tr>
<td>SPI, one channel</td>
<td>SPI communication interface</td>
<td>0.040</td>
<td>0.251</td>
<td></td>
</tr>
<tr>
<td>I2C bus</td>
<td>Renesas Inter Equipment Bus</td>
<td>0.059</td>
<td>0.372</td>
<td></td>
</tr>
<tr>
<td>OPC</td>
<td>OPC calculation module</td>
<td>0.003</td>
<td>0.021</td>
<td>used for diagnosis</td>
</tr>
<tr>
<td>RTC &amp;</td>
<td>Real-Time Clock module</td>
<td>0.148</td>
<td>0.328</td>
<td></td>
</tr>
</tbody>
</table>

## Safety mechanisms considered for each element

- FIT rates for both permanent & transient failures modes

© 2014 Renesas Electronics America. All rights reserved.
RX Safety Plan Platform Scalability

- RX700 (240 MHz): Leading edge performance, up to 8MB Flash and 512kB RAM.
- RX640 (120 MHz): High performance, integration, up to 8MB Flash and 512kB RAM.
- RX600 (100 MHz): High performance, integration, up to 2MB Flash and 256kB RAM.
- RX200 (50 MHz): Low power, up to 1MB Flash and 96kB RAM, without FPU.
- RX100 (32 MHz): Low power, cost effective, up to 128KB without FPU.

SW Self-Test covers RX600, RX200, and RX100 family groups.
Synergy Provides Internal Safety Functions

Safety Certification Is Part of Product Plan

Note: Not all features are on all devices
IoT Networking
Connectivity That Links Time Domains

- Real-time and non-realtime domains
- Intelligent gateways partition between factory and enterprise
- Secure-cloud based connectivity
- Multiple protocols and standards
Solutions For Industrial IoT Networking

- Multi-protocol support
- Hardware accelerators
  - License free EtherCAT & CCLink IE
- Single/Dual Channel Ethernet
- Ethernet DMAC
- Cut-through, Store & Forward

- RIN32M3
- TPS1
- Soft Real Time
  - 1 to 100ms Cycle Time
- Non-Real Time
  - 10 to 100ms Cycle Time
- Sensor Networks
R-IN32M3-EC Block Diagram

Supports Multiple Protocols

EtherCAT
EtherNet/IP
MODBUS-IDA
CANopen
CC-Link IE

128 bits Hardware Function Bus

Hardware Function Control
Header Endpoint
Buffer RAM with ECC 64KB
Buffer Allocator
INT DMA
MAC DMA
Ether MAC

128 bits Communication Bus

Debug
Cortex-M3 CPU
NVIC
Hardware Real-time OS
Data RAM with ECC 512KB
AHB2DMA

AHB-Lite Multi Layer Bus Sub-System

Real-time Port DMAC
General DMAC 4ch
Real-time Port
General Port
CC-Link
Serial Flash MEMC
ROM/ SRAM MEMC
Host CPU Interface
Inst. RAM with ECC 768KB
Inst. RAM

APB

Timer Array
UART x2
IIC x2
CAN x2
CSI x2
WDT
Outline of R-IN32M3 RTOS In Hardware

Traditional SW-RTOS

- Resource management, queuing, task schedules, context switching, etc. all done in software
- Dependent on CPU loading
- Not deterministic for real-time industrial applications

R-IN32M3 RTOS operation in Hardware

- Familiar SW RTOS environment (Micrium’s uC/OS-III HW-RTOS)
- OS library for system call commands and dispatch only
- Task scheduling and queuing function in hardware
- Up to 30 System Calls: Events, Semaphores, Mailbox operation, etc.
Synergy S7 Dual Ethernet Controller

- Two integrated Ethernet MACs, 10/100 Mbps
- IEEE 802.3x-compliant flow control (MII/RMII)
- Supports IEEE 1588v2 PTP
- Dedicated Ethernet DMA controller for data transfer without CPU intervention
- Supports full-duplex and half-duplex transfer modes
- Supports Magic Packet™ detection and Wake-on-LAN (WOL) functionality
Security in Industrial IoT
Cyber Attacks Happens Every Second

http://map.norsecorp.com/

Cyberattack on German Steel Plant Caused Significant Damage: Report
By Eduard Kovacs on December 18, 2014

An attack launched by an advanced persistent threat (APT) group against an unnamed steel plant in Germany resulted in significant damage, according to a new report.
Security Awareness Levels & Mitigation Measures

- **Device Level**
  - Access Control

- **System Level**
  - Context Aware

- **Perimeter-Centric**
  - Perimeter

- **Pervasive**
  - Threat Aware

**Device Level Mitigation Measures**
- Key management
- Secure network protocols
- Firewalls
- Data encryption
- Authentication of data sources
- Hardware-assisted control-flow monitoring

**System Level Mitigation Measures**
- Security analytics
- Context aware application software
- Cyber integrity
- Product lifecycle management
- Business process

Source: Cisco, 2013
Objectives of a Security Solution

- Secure Boot
- Secure encrypted communication
- Authentication
- Protection against cyber attacks
- Secure Code Updates
- Data Security
- Intrusion detection & security monitoring
Cloud Connectivity Needs Secure Connection

Typical Plant Cloud Structure

Users request the data from Industrial Control System (ICS)

Requires open firewall ports

- Typically VPN connections are used
- Need for login/logout

VPN provides secure path but not secure from data tampering, sniffing or hacking
Embedded Agent Eliminates Attack Surface

Initial connection to the cloud server is outbound from the device
- Yet full bi-directional communication

All inbound firewall ports remain closed
- No internet attack surface
- No need for VPNs

Users have access to the data, but not the plant network
- No risk of virus propagation, as each connection is isolated and unique
Secure, Real-Time Data In SaaS Model

Real-time performance

- Supports data updates in msec and 50,000 data point changes per second
- Supports redundant connections with hot swap over capability
- Connect to OPC, Excel, Databases and many other protocols

Real-time HMI in-plant and remotely

- Mirror the capability of real-time performance
- 4,000+ image library

Simple service model
Challenges in Developing IIoT Device Security

IIoT Edge devices are embedded devices

- Embedded RTOS-based (Linux, ThreadX, uC/OS III, etc.)
- Limited resources for security software
- Traditional IT security solutions won’t work

Not just about data

- Maintain operation integrity
- Limited or no downtime allowed
- Remote access

Need solution designed for embedded devices

- Make or Buy decision
Device Level Security for IIoT Edge Applications

- Data security prevents unauthorized access to the device
- Authentication and protection against cyber attacks
- Intrusion detection and security monitoring
- Building blocks for compliance with security standards including EDSA, ISA/IEC 62443 and NIST guidelines
- Portable, small footprint; Minimal performance overhead
- Icon Labs' Floodgate Security Framework and Floodgate Security Manager business model simplifies deployment
Synergy’s Security In Hardware

Flash Area Protection
- Write-protects an area within the code flash to prevent undesired self-programming

Synergy Secure Crypto Engine
- 128-bit unique Identification per device
- True RNG (TRNG)
- AES and data encryption
- Cryptographic Hash functions

Secure Boot Function*
- Boot loader will authenticate User Application binary to ensure that is authentic/ has not been tampered with

* Software solution licensed separately
IIoT Analytics by Functional Domain

Control Domain

- Sensor data Validation
- Real-time Monitor & Diagnosis
- Safety/Security analysis
- Descriptive analytics

Operations Domain

- Provisioning/Deployment
- Prognostics & Optimization
- Process Monitor & Diagnosis

Information Domain

- Ingestion & transformation
- Streaming & Batch analytics
- Contextual security
- Predictive analytics

Business Domain

- Business Analytics
- Decision Support Services
- Decisive Analytics

Real-time Region

Edge Gateway

Data Services

Analytics

Meta Data & Storage

Reference: IIoT Reference Architecture, IIC

Reference: IIoT Reference Architecture, IIC
Edge Analytics Using Industrial Sensor MCUs

- **Temperature/Pressure Sensors**
  - 24-bit ΔΣ ADC
  - 16-bit ΔΣ ADC w/ sensor Amp
  - 12-bit SAR
  - 10-bit SAR

- **Proximity Sensors**; Inductive, capacitive
  - 14-bit SAR
  - 12-bit SAR
  - 10-bit SAR

- **Flow Sensors**
  - 24-bit ΔΣ ADC
  - 16-bit ΔΣ ADC w/ sensor Amp
  - 12-bit SAR

- **Ultrasonic Sensors**
  - 14-bit SAR
  - 12-bit SAR

- **Conductivity sensors**
  - 10-bit SAR

- **ADC Resolution (bits)**
  - 24
  - 16
  - 14
  - 12
  - 10
  - 8

- **Sampling rate (samples/sec)**
  - 24
  - 16
  - 14
  - 12
  - 10
  - 8

- **Sampling rate**
  - 24-bit ΔΣ ADC: 1.4 MSPS
  - 16-bit ΔΣ ADC w/ sensor Amp: 2.5 MSPS
  - 12-bit SAR: 470ksps
  - 10-bit SAR: 1.4 MSPS
  - 8-bit SAR: 2.5 MSPS
Event Link Controller (ELC)

Allows direct interaction between different modules without CPU intervention
Routes source events generated by a peripheral to event inputs on other peripherals
Event signal can activate a peripheral for the desired operation

- Start/stop/clear timer, up/down counting
- Start ADC and DAC conversion
- Start Captouch measurement
- Start DMA/DTC transfer
- Issue interrupts to the CPU
- Change state of GPIOs

Most peripherals generate event signals
Industrial IoT Is Expanding Value Chain

Expanding Traditional Business

Data Analytics
Cloud Security
Analytics Integration
Cloud SaaS

Enterprise Services
Factory SW/Eqpt
System Integrators
Industrial OEM
Embedded HW/SW
Middleware
Silicon

Factory-Enterprise HW
Software analytics
Cloud Connectivity
Ready to use hardware
Safety & security integrated

© 2015 Renesas Electronics Corporation. All rights reserved.
Revenue Services Resulting From Industrial IoT

- Safety certified modules, sensors, controllers
- Industrial network protocols
- Sensor & Actuator analytics
- Secure remote upgrade from trusted sources
- Device to Fog connectivity

Big Data Management
- IT/OT Integration
- Data As An Asset
- Enterprise to Mobile Connectivity

Enhancement Services
- Predictive Maintenance
- Systems Performance
- Closed loop Product Lifecycle Management
- Process Analytics
- Process Visualization
- Provisioning & Key Management
- Process to Cloud Connectivity

Start At The Edge

Fog Data

© 2015 Renesas Electronics Corporation. All rights reserved.
Summary
Industrial IoT Summary

Industrial IoT will reshape manufacturing of the future

- Collaborative and self-managing machines
- Big Data with cloud connectivity
- Context based analytics
- Security and safety at every level

Intelligent sensors and digital devices

IIoT Solutions Start at the *Edge*

- *Accelerate* designs with systems on chip solutions and pre-certified software
- *Innovate* by leveraging a platform that provides edge to cloud connectivity
- *Differentiate* with better security, analytics and new business models