Dissecting the Internet of Things

Speakers:
Andrew Caples, Product Marketing Mgr - Embedded SW, Mentor Graphics
Dr. Edwin de Jong, Vice President of Sales, RTI
Varun Nagaraj, Senior VP & GM, Internet of Things, Echelon Corp.
John Blevins, Director of Product Marketing, LynuxWorks

Moderator:
Curt Schwaderer, Technology Editor, OpenSystems Media
Agenda

- Housekeeping
- Presentation
- Questions and Answers
- Wrap-up
Internet of Things
Vision of Smart, Intelligent Connections

Andrew Caples
Sr. Product Marketing Manager, Nucleus RTOS

mentor.com/embedded
Its going to be BIG!

Source: Company Data, Thomson Reuters, Morgan Stanley Research
What is IOT?
What is IOT?

Open fridge – remind me to track food eaten
What is IOT?
What is IOT?
What is IOT?
Security
Coming soon…
Zero Configuration

Devices are added to the network without user intervention
“The Next Big Thing is actually a Trillion Small Things. Networked microcontrollers with sensors and actuators are about to be embedded in any tangible object or place, ready to observe and control the real world. Imagine tiny web servers in all embedded devices, ready to connect to the Internet and provide their observations and services to a new set of Web applications. Ericsson has a vision of 50 billion connected devices by 2020. Included in this vision is the Networked Society where all aspects of people's lives, the operations of enterprises and society in general are impacted by the proliferation of communications. The Internet of Things will be a major cornerstone of an emerging networked society.” – Ericsson, Ericsson Labs
https://labs.ericsson.com/research-topics/internet-of-things

http://research.cens.ucla.edu/projects/2005/NIMS/coordinated_mobility/
# Nucleus RTOS for IoT

## Additional Middleware

<table>
<thead>
<tr>
<th>Technology</th>
<th>Functionality</th>
<th>Technology</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEP 2.0/ OpenADR</td>
<td>IPSec / IKE</td>
<td>SNMP v1/v2/v3</td>
<td></td>
</tr>
<tr>
<td>XML / JASON</td>
<td>SSL / CyaSSL</td>
<td>HTTP Server / Client</td>
<td></td>
</tr>
<tr>
<td>SAFE/ FAT File System</td>
<td>SSH</td>
<td>DHCP</td>
<td></td>
</tr>
<tr>
<td>Graphics</td>
<td>WPA Supplicant</td>
<td>DNS-SD / mDNS</td>
<td></td>
</tr>
<tr>
<td>SQLite</td>
<td>WebSockets</td>
<td>FTP / TFTP / Telnet</td>
<td></td>
</tr>
</tbody>
</table>

## Middleware

<table>
<thead>
<tr>
<th>Technology</th>
<th>Functionality</th>
<th>Technology</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB 2.0/3.0 /OTG</td>
<td>IPv4 / IPv6</td>
<td>802.11 /802.1x</td>
<td></td>
</tr>
<tr>
<td>6LowPAN</td>
<td>CoAP</td>
<td>RPL</td>
<td>Bluetooth/BLE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zigbee</td>
</tr>
</tbody>
</table>

## Kernel Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Management</td>
<td></td>
</tr>
<tr>
<td>Device Manager</td>
<td></td>
</tr>
<tr>
<td>Processes</td>
<td></td>
</tr>
</tbody>
</table>

**Nucleus RTOS**
RTI Overview

Communications Intelligence for The Internet of Things
The Internet of Things

- Personal mobile
- Global connectivity
- Digital society Sustainable world

Inflection points

THINGS 50 billion
PEOPLE 5 billion
PLACES 1 billion
What is the Internet of Things?

- Cisco “Internet of Everything”
  - ...the latest wave of the Internet -- connecting physical objects...to provide better safety, comfort, and efficiency

- IBM “Internet of Things”
  - ...a completely new world-wide web, one comprised of the messages that digitally empowered devices would send to one another. It is the same Internet, but not the same Web.

- GE “Industrial Internet”
  - ...convergence of machine and intelligent data...to create brilliant machines

- RTI “Your Systems. Working as One.”
  - ...an entirely new utility. As profound as the cell network, GPS, or the Internet itself. The Internet of Things and the Intelligent Systems it enables will fundamentally change our world.
What Connects The Things?

- **Access**
  - Link sparse endpoints
  - XMPP

- **Process**
  - Biz intelligence
  - Centralized/ESB
  - ~100ms
  - MQ/AMQP

- **Collect**
  - Collect data
  - Hub & spoke
  - ~10ms
  - MQTT/CoAP

- **Control, distribute**
  - DataBus
  - ~.01ms
  - DDS
DDS: Distribute Device Data

Data Distribution Service (DDS)
Smart Things

© 2013 Real-Time Innovations, Inc.
Raytheon uses RTI middleware to control the new Zumwalt DDG 1000 destroyer.

RTI DDS coordinates and manages complex, diverse onboard hardware and software systems.

RTI connects hundreds of computers, thousands of applications, and more than 10m publish-subscribe pairs.

RTI middleware extends real-time scalability.
EMS Cloud Integration

Connecting devices with hospitals to provide better treatment while en-route
Hospital Patient Safety

• Hospital error is the 6th leading cause of preventable death

• RTI Connext DDS ties together devices, services, and displays in real time

• Integrated DocBox decision engine improves patient safety

“RTI Connext DDS met all our needs – whether we’re handling 12 patients, or 200.”

-- DocBox Founder, Tracy Rausch
High Rate Distributed Control

- The Minimally Invasive Robotic Surgery (MIRS) system at DLR coordinates three robots to perform delicate heart surgery.
- The system closes a distributed loop between the robots and the remote surgeon’s control at 3kHz.
- RTI enables new medical techniques
Space-Proven Data Link

• NASA’s Human-Robotic Systems prototypes robots for extraterrestrial surfaces

• NASA uses DDS for low-bandwidth, high-delay, lossy space-earth communications from the ISS

• RTI middleware communicates over disadvantaged links
Harsh Environment Operations

• Joy Mining is the world’s largest mining equipment manufacturer
• DDS connects the controller, operator GUI, and historian
• Reliable, fast connectivity enables control, debugging, and system health monitoring for continuous mining
The Industrial Internet of Things (IIoT)

January 2014
Echelon: Control Networking Pioneer

1988
Founded by AC Markkula

1988
IPO on NASDAQ

1990
Launched LonWorks™ control networking platform

1990
Enel licenses platform for 30M+ smart meters

1998
LonWorks control networking platform

1998
Launch

1998
IPO on NASDAQ

2000
Honeywell selects platform for building automation

2000
Philips selects platform for street lighting

2000
1st utility to embrace smart grid solution platform

2005
Duke Energy commits to platform

2008
Philips selects platform for street lighting

2008
Honeywell selects platform for building automation

2008
Honeywell selects platform for building automation

2008
Enel licenses platform for 30M+ smart meters

2009
Duke Energy commits to platform

2010
First China street light win

2011
Siemens ships 1M room controllers

2013
Industrial Internet Of Things

110M+
Devices shipped

- Buildings
- Lighting
- Industrial
- Transportation
- Grid

2013
VATTENFALL

28
Control Networking is Transitioning

From Control Networking 1.0 to the Industrial Internet of Things (IIoT)

IIoT is
- Control Networking 1.0 + IP + Wired/Wireless + Multiple Protocols + Big Data + Cloud
- IP-to-the-end point (in the field bus), and less use of Gateways

Why IP-based control networking is inevitable

- Big Data queries require dynamic access to all small data
- IT organization will be more involved in automation networks
- OEMs will need to add support for many links and many protocols

- Native IP devices are better fit than static gateways for analytics
- IP devices integrate with existing operational IT frameworks
- IP in device simplifies development framework
IloT will be Large and Different

More Industrial IoT Devices than Consumer IoT or Smart Phones by 2020!

Key IloT Segments

More Wired than Wireless in Industrial Segments!
IIoT Requirements are Unique

Autonomous Control
Doing, not just talking: Minimal human interaction, autonomous peer-to-peer communities

Industrial-strength Reliability
Must work in the face of noise, node failure, local network failure, internet connectivity failure

Legacy Co-existence and Evolution
Brownfield, not Greenfield: Wired and wireless connectivity, existing multi-drop wiring, multiple control protocols over IP

Hardened Security
Compromised IP device is not an option

IIoT Devices and Applications
Need a Different Platform than Generic/Human IoT Devices and Applications that can reduce development time and lower risk
One Example of IIoT Being Different

Are IIoT Environments Connected Differently?

- IIoT wiring options
  - Structured / star topology
  - **Multi-drop**: Ring, loop, bus
- Why not Ethernet?
  - Great for structured / star wiring
  - Costly and sub-scale for multi-drop
- Why not RS 485?
  - Hard to install correctly
  - No longer low cost if required to handle IP traffic interrupts
- Why FT
  - All topology types
  - Simple to install and expand network: Polarity insensitive (except ring); only one terminator anywhere on segment
  - Highest noise immunity
  - Dedicated processor for IP interrupt handling
Device Control Points create a peer-to-peer control fabric.

- Discovery
- Secure group messaging
- Bindings / associations
- Device profiles
- Programming environment

Resilient Community of Devices

Device Control Points could be:

- System-on-chip
- Modules
- Stacks on any processor

Platform should also include Routers, and Management Software
Echelon’s IzoT™ Platform for IIoT

The IzoT Platform Adds:

- IP-enabled SOCs for wired connectivity
- Modules for wireless
- IP-based stacks for host processors
- Multi-protocol support on-chip (Initially BACnet)
- Border routers for IP address management
- Next generation gateways
- REST Interfaces
- IP-based Commissioning and Management
- Cloud-based delivery option
Keeping Your World Safe and Secure

Security and the IoT

John Blevins
Director, Product Marketing
LynuxWorks, Inc.
San Jose, California, USA
jb@lnxw.com
Connected Embedded Devices

- Much key industrial and commercial infrastructure is now controlled by embedded devices

- These embedded devices are changing… They are now:
  - Connected to the internet and each other using:
    - Long haul networks
      - TCP/IPv4, IPv6, 2G/3G/4G cellular, WiMax
    - Short haul networks
      - WiFi, Zigbee, Bluetooth
  - Evolving from small, proprietary, purpose built OS’s to suddenly requiring networking and security
  - Often using general purpose Os’s (Windows, Linux, Android) to help with GUI, connection, applications, etc.
    - And hence becoming more vulnerable to the cyber threats that traditionally attack our computers and mobile devices

- RTOS’s & secure Hypervisors for next-generation connected devices must facilitate secure communication and access
More and more of the world’s industrial infrastructure is controlled by connected computers. E.g. Industrial automation, medical systems, power generation & distribution, smart grid.

Cyber attacks on the central control systems could bring a city, region or country to a standstill.

Facilities are well protected from physical attack, but less so from a cyber attack.

- Currently use the same network protection and operating systems as commercial enterprise.

Malware has become very sophisticated in its entry, infection and damage mechanisms.

- E.g. Stuxnet Worm.
Approaches to Security

● Prevent Infiltration
  – Keeping attackers out - hasn’t worked …

● Prevent Exfiltration
  – Prevent loss of sensitive data – hasn’t worked either ….

● Separation of data
  – Compartmentalize data to better protect it

● Defense-in-Depth
  – Have multiple layers of security
  – If one fails… the other succeeds
Layered Security Approach

- Adding security in depth is key to protecting our critical systems
  - RTOS Security
    - A modern RTOS can be used to add layers of military grade security to both the OS & application levels
  - Separation Kernel / Hypervisor
    - Advanced virtualization technology can add security below the OS
LynxOS Family of Security RTOS

- LynxOS-178 – Safety Critical DO178B Certified Partitioning RTOS
  - Each partition has its own resources (time budget, memory allocation, I/O devices, etc) and software applications.
  - Applications in one partition cannot interfere with another partition’s resources or the correct operation of its software applications.
  - Health Monitor

- LynxOS – Military Grade Security RTOS
  - Full SMP support, POSIX based hard real-time OS
RTOS Security Features

- Discretionary Access Control
- Audit
- Roles & Capabilities Privileges
- Identification & Authentication
- Cryptography
- Quotas
- Self-Test
- Residual Information Protection
- Trusted Path
Separation Kernel / Hypervisor

- Separation Kernel technology has become the standard approach for providing the highest levels of security on a single system.
- Separation of multiple guest Os’s can be hosted on a single physical system using virtualization of cpu, disk, network and other devices.
- Can work on sensors, edge devices, concentrators and servers.
- Non-secure operating systems and their applications can now be run on the same physical system as secure applications.
A Separation Kernel runs under the OS or RTOS and can detect and protect against zero-day rootkit & bootkits – the worst kind of malware.
Security Layers - Defense in depth

- By combining a Separation Kernel with a military grade, highly secure RTOS, connected M2M systems will have true multi-layer security.

- The IOT Revolution can then proceed with the knowledge that it’s soft underbelly is no longer exposed to cyber threats.
Audience Q & A

Andrew Caples
Embedded SW Product Marketing Mgr
Mentor Graphics

Dr. Edwin de Jong
Vice President of Sales
RTI

Varun Nagaraj
Senior VP & GM, Internet of Things
Echelon Corp.

John Blevins
Product Marketing Director
LynuxWorks
Thanks for joining us

Event archive available at:

http://ecast.opensystemsmedia.com/

E-mail us at: clong@opensystemsmedia.com