Safety and Security Concerns in Vehicle Connectivity and Autonomous Driving: Can Ethernet Play a Role?

IEEE Ethernet & IP @ Automotive Technology Day

Nancy Cam-Winget
Distinguished Engineer, Cisco Security Business Group

November 2017

The Security Challenge

TREND MICRO
TrendLabs SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS
Home
Categories
186
865

Home » Exploits » The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard

The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard

Posted on: August 16, 2017 at 5:00 am **Posted in:** Exploits, Internet of Things
Author: Federico Maggi (Senior Threat Researcher)

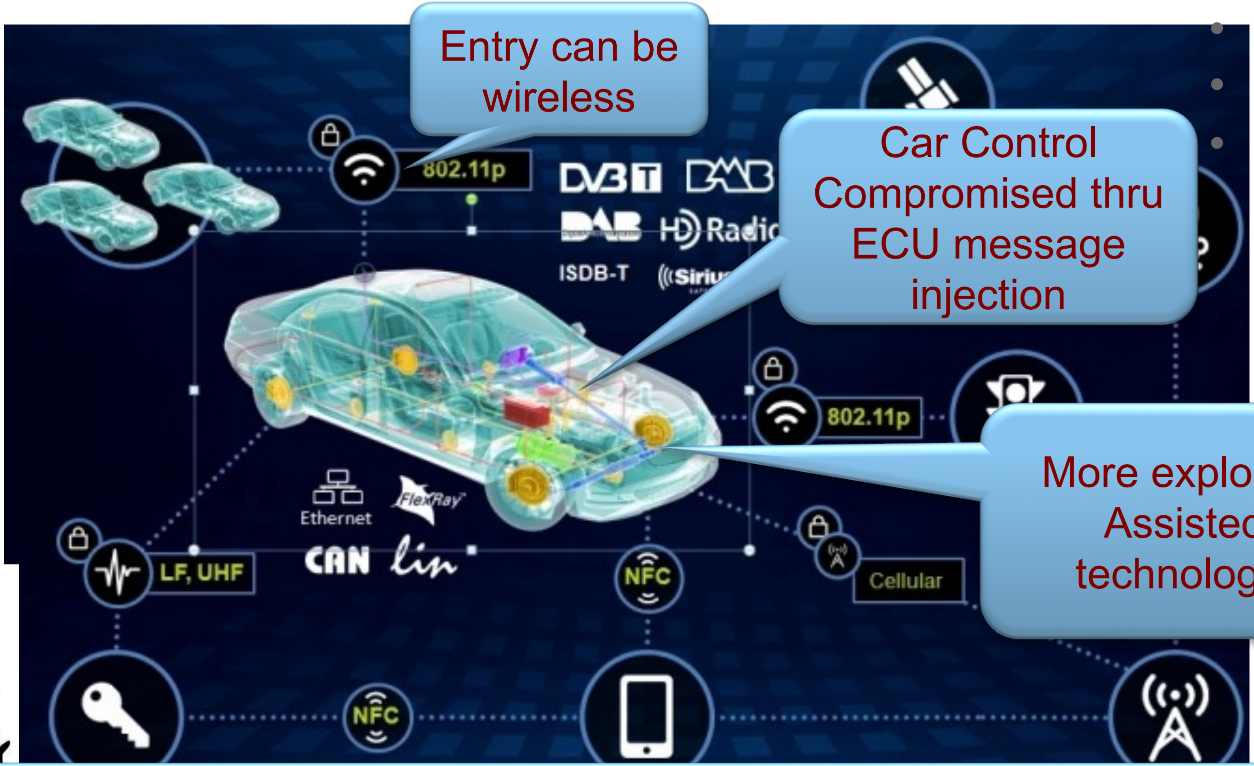
In many instances, researchers and engineers have found ways to hack into modern, internet-capable cars, as has been documented and reported several times. One famous example is the Chrysler Jeep hack that researchers Charlie Miller and Chris Valasek discovered. This hack and those that have come before it have mostly been reliant on specific vulnerabilities in specific makes and/or brands of cars. And once reported, these vulnerabilities were quickly resolved. But what should the security industry's response be when a hack is found that is not only successful in being able to drastically affect the performance and function of the car, but is also stealthy and

ANDY GREENBERG SECURITY 08.16.17 04:55 PM

A DEEP FLAW IN YOUR CAR LETS HACKERS SHUT DOWN SAFETY FEATURES

Attacks on Vehicles

Trends:
- Increased # ECUs
- Assisted driving
- WiFi Hotspot
- OTA



Entry can be wireless

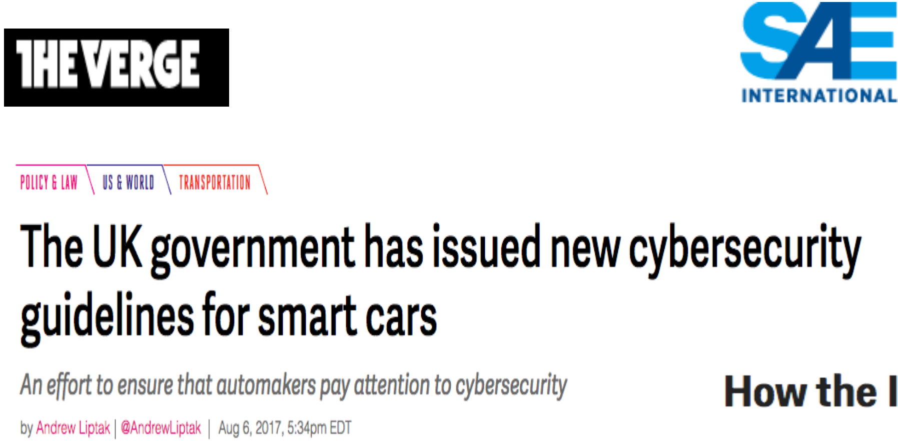
Car Control Compromised thru ECU message injection

More exploits to come: Assisted Driving technology [DSRC]

Car Hacking Guide: http://illmatics.com/Remote%20Car%20Hacking.pdf

Image source:https://opentechdiary.wordpress.com/tag/connected-things/

Challenges Towards Securing Vehicles

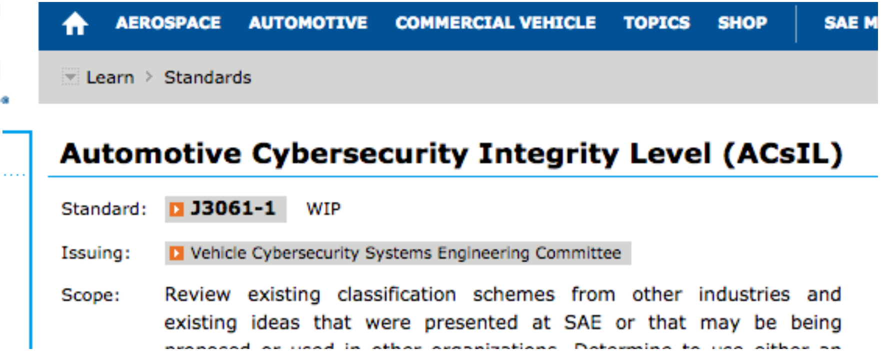


THE VERGE

The UK government has issued new cybersecurity guidelines for smart cars

An effort to ensure that automakers pay attention to cybersecurity

by Andrew Liptak | @AndrewLiptak | Aug 6, 2017, 5:34pm EDT



Automotive Cybersecurity Integrity Level (ACsIL)

Standard: J3061-1 WIP

Issuing: Vehicle Cybersecurity Systems Engineering Committee

Scope: Review existing classification schemes from other industries and existing ideas that were presented at SAE or that may be being proposed or used in other organizations. Determine to use either an

How the Internet of Things will affect security & privacy

Andrew Meola

Dec. 19, 2016, 2:43 PM 66,299

; more

We're entering the world of invisible technology. Can we keep up?

Bob O'Donnell, Special for USA Today Published 6:00 a.m. ET July 4, 2017 | Updated 11:04 a.m. ET July 4, 2017

FOSTER CITY, Calif. — It's a well-proven fact in the tech world that timing is everything

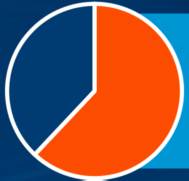
Thank you.

2017 IEEE Standards Association (IEEE-SA)
Ethernet & IP @ Automotive Technology Day

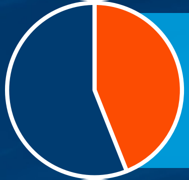
Panelist: Kevin Stanton

The State of Security in the Connected Car

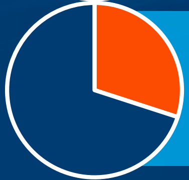
Consumers are nervous about connected-car security[1]**:**



62% Worry about connected cars being easily hacked



44% Believe the automaker is most responsible for securing a vehicle



30% Say software and app makers are most responsible for security

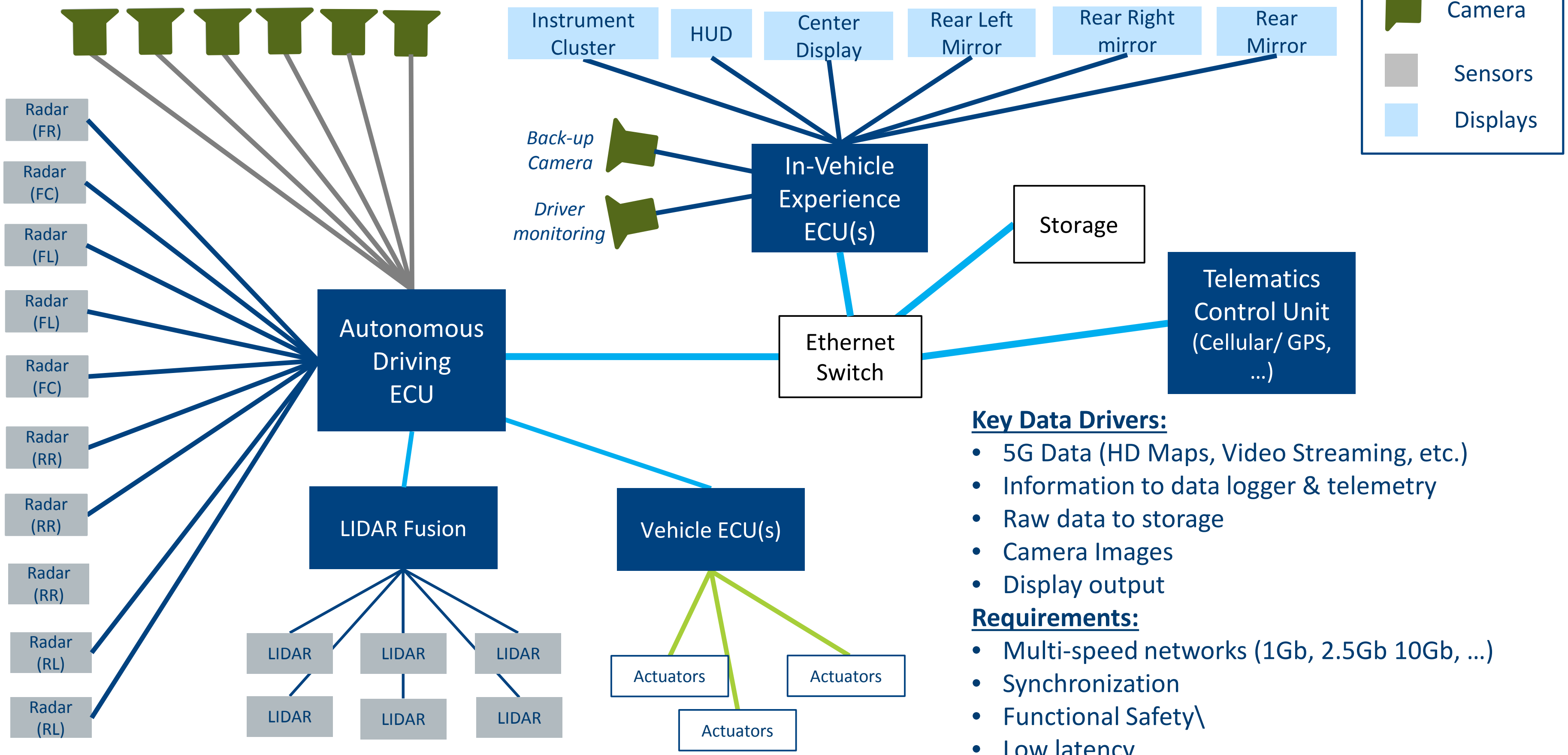
Gartner predicts that by 2019, two automotive companies will be fined for vehicle software design negligence that results in inconsistent technology performance or cybersecurity attacks.[2]

The Security and Privacy in Your Car (SPY Car) Act of 2017 would require regulations to protect cars from unauthorized access to electronic controls and data.

Ripped from the headlines
In 2016, one security researcher showed that he could compromise a vehicle's lidar sensor with a device he assembled for just $43 and a laser pointer.[3]

1. "Braking the Connected Car: The Future of Vehicle Vulnerabilities," ~ Kelley Blue Book, March 2016.
2. *"Staying on Track with Connected Car Security,"* ~ Gartner, February 2016.
3. *"Self-driving cars are prone to hacks—and automakers are barely talking about it,"* ~ Business Insider, December 2016.

Automotive Networking



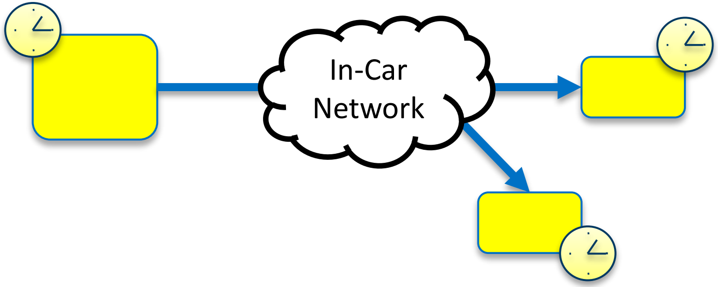
Key Data Drivers:

- 5G Data (HD Maps, Video Streaming, etc.)
- Information to data logger & telemetry
- Raw data to storage
- Camera Images
- Display output

Requirements:

- Multi-speed networks (1Gb, 2.5Gb 10Gb, …)
- Synchronization
- Functional Safety\
- Low latency

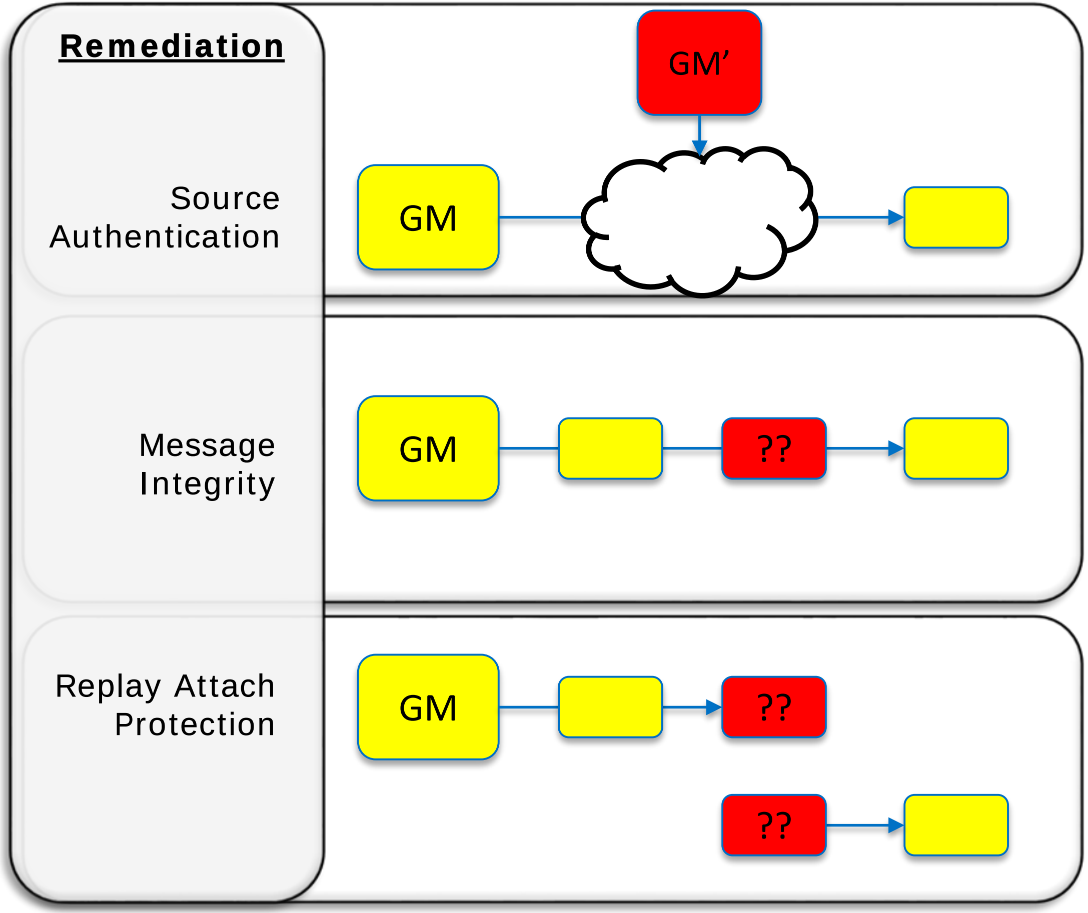
Typical Network Time Transfer using TSN (PTP/802.1AS)



All’s Well

Bad Guy

Some Threats to Network Time Transfer

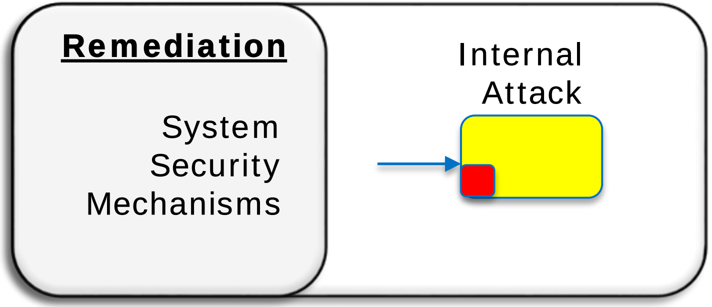


Remediation

Source Authentication

Message Integrity

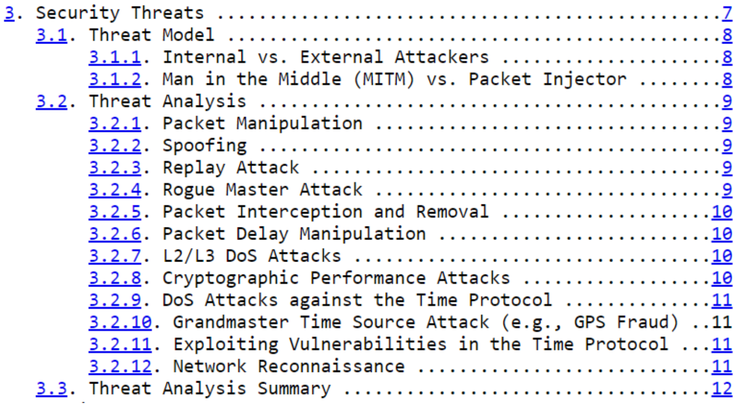
Replay Attach Protection



Remediation

System Security Mechanisms

Internal Attack



https://tools.ietf.org/html/rfc7384

ETHERNET ARCHITECTURES

THOMAS HOGENMÜLLER

Ethernet Architectures

Future Mobility: Electrified, Automated and Connected

costs hybrid e-motor

eBike power electronics

electrified

plug-in eScooter range

fun-to-drive battery

charging infrastructure

legislation driver assistance

emergency braking autopilot

automated

highway-pilot sensors

redundancy electric steering

valet parking

electronic horizon

smartphone integration

connected

eCall cloud

services fleet management

car2car augmented reality

Ethernet Architectures

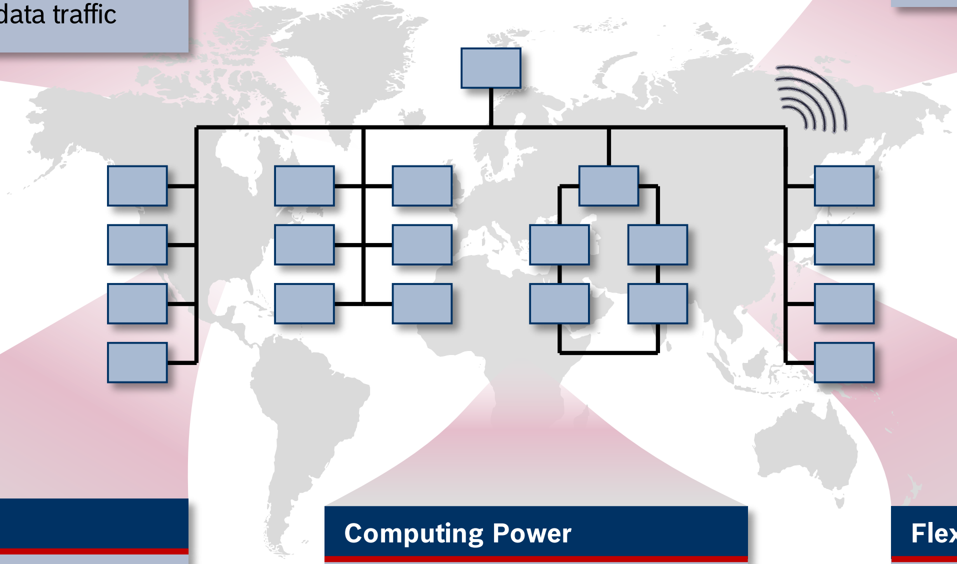
Bottlenecks of Today's E/E Architectures

Communication Bandwidth

Inter-domain and cross-domain **communication bandwidths** not sufficient for future data traffic

External Communication

Lead to higher data traffic and significant **security risks**



Scalability

Many segments, markets and technologies leading to complex, and expensive **variant handling**

Computing Power

Serial computing in embedded systems is hitting the **technological limits**

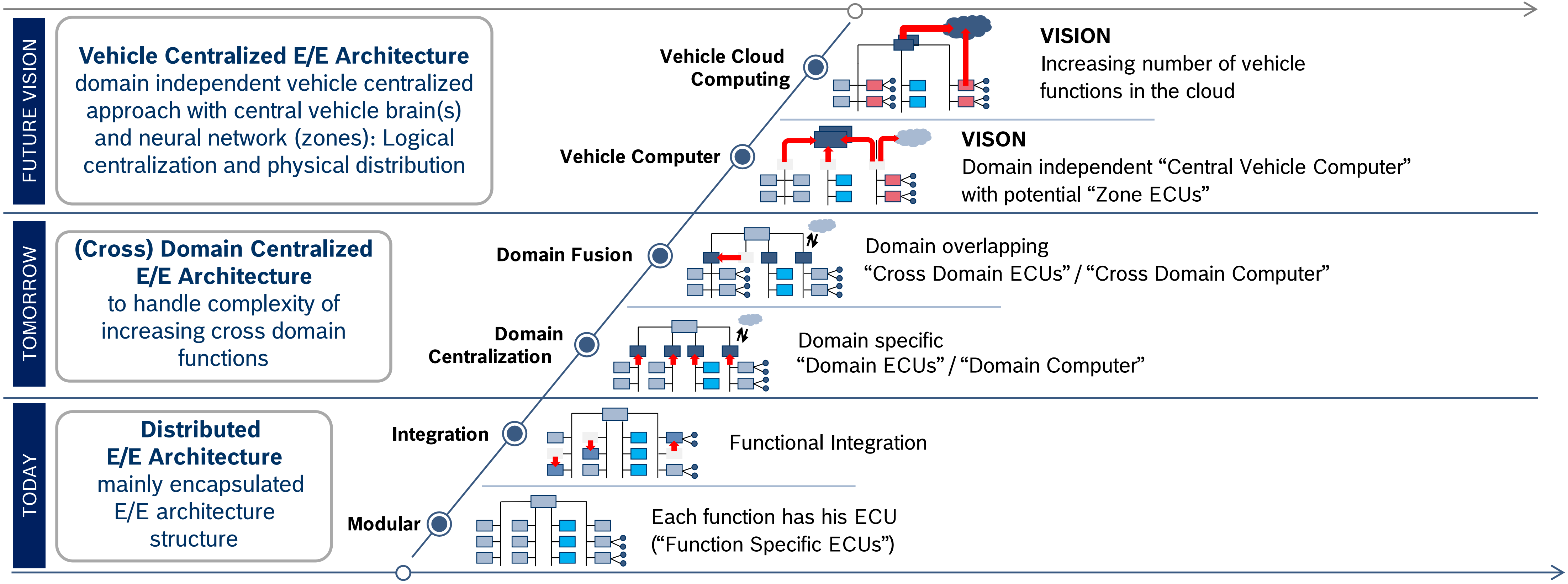
Flexibility

Future E/E systems need to allow swift **introduction of new innovations & SW sharing**

Ethernet Architectures
E/E Architecture Roadmap: Centralization

Under discussion AD-vehicles

Up to 400 Ethernet ports per car (100 M, 1000 M, 10 G, >10 G)



FUTURE VISION

Vehicle Centralized E/E Architecture
domain independent vehicle centralized approach with central vehicle brain(s) and neural network (zones): Logical centralization and physical distribution

TOMORROW

(Cross) Domain Centralized E/E Architecture
to handle complexity of increasing cross domain functions

TODAY

Distributed E/E Architecture
mainly encapsulated E/E architecture structure

Vehicle Cloud Computing

VISION
Increasing number of vehicle functions in the cloud

Vehicle Computer

VISON
Domain independent “Central Vehicle Computer” with potential “Zone ECUs”

Domain Fusion

Domain overlapping
“Cross Domain ECUs” / “Cross Domain Computer”

Domain Centralization

Domain specific
“Domain ECUs” / “Domain Computer”

Integration

Functional Integration

Modular

Each function has his ECU
(“Function Specific ECUs”)

increasing SW amount

▭ typ. state of the art automotive ECUs (function specific)

■ Performance ECUs (e.g. Domain ECU /Central ECU/Vehicle Computer)

⬚ Optional ECUs

🟥 Domain independent Zone ECUs

< Sensors/Actuators

ECU = Electronic Control Unit

🟦 Domain specific Zone ECUs (e.g. todays Door ECU)

nebbiolotechnologies
fog computing pioneers

A Few Thoughts on Real Time and Converged Control Architecture

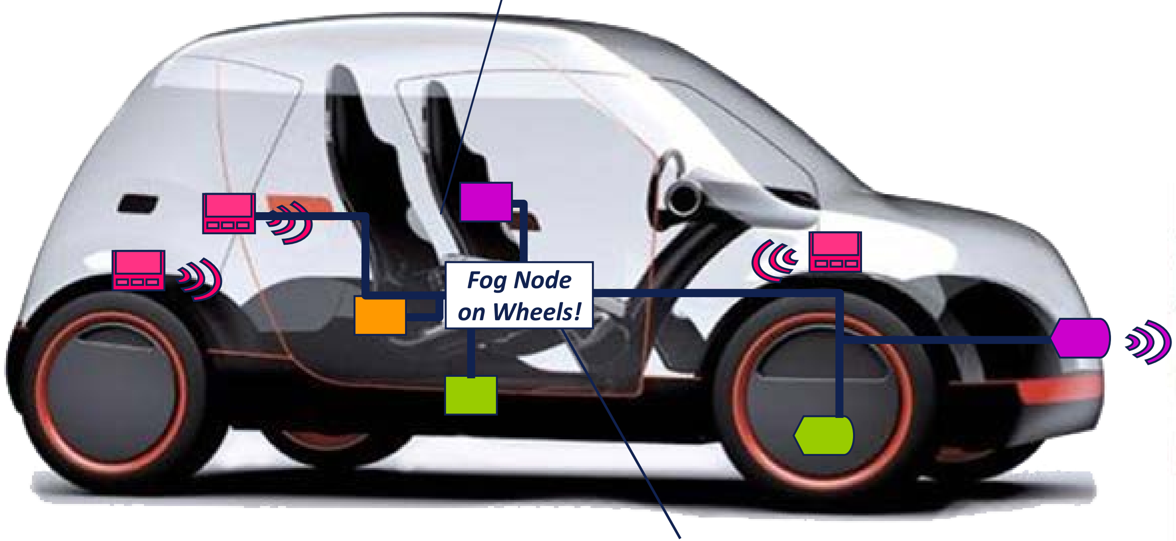
Flavio Bonomi, CEO and Co-Founder, Nebbiolo Technologies

November 1st, 2017

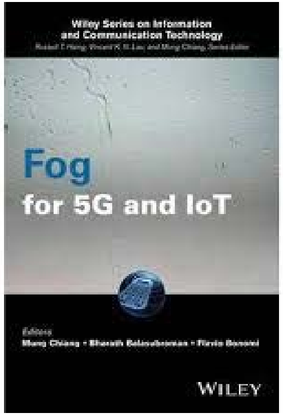
The Role of Fog Computing in the Automobile Evolution

The Future Car Domain Controller is a Fog Node! (Ricky Hudi, former Audi Head of Electronics)

Deterministic Ethernet Network and Consolidated, Virtualized ECU "Data Center"



Central Gateway



Wiley Series on Information and Communication Technology
Fog
for 5G and IoT
Editors
Mung Chiang • Bharath Balasubramanian • Flavio Bonomi
WILEY

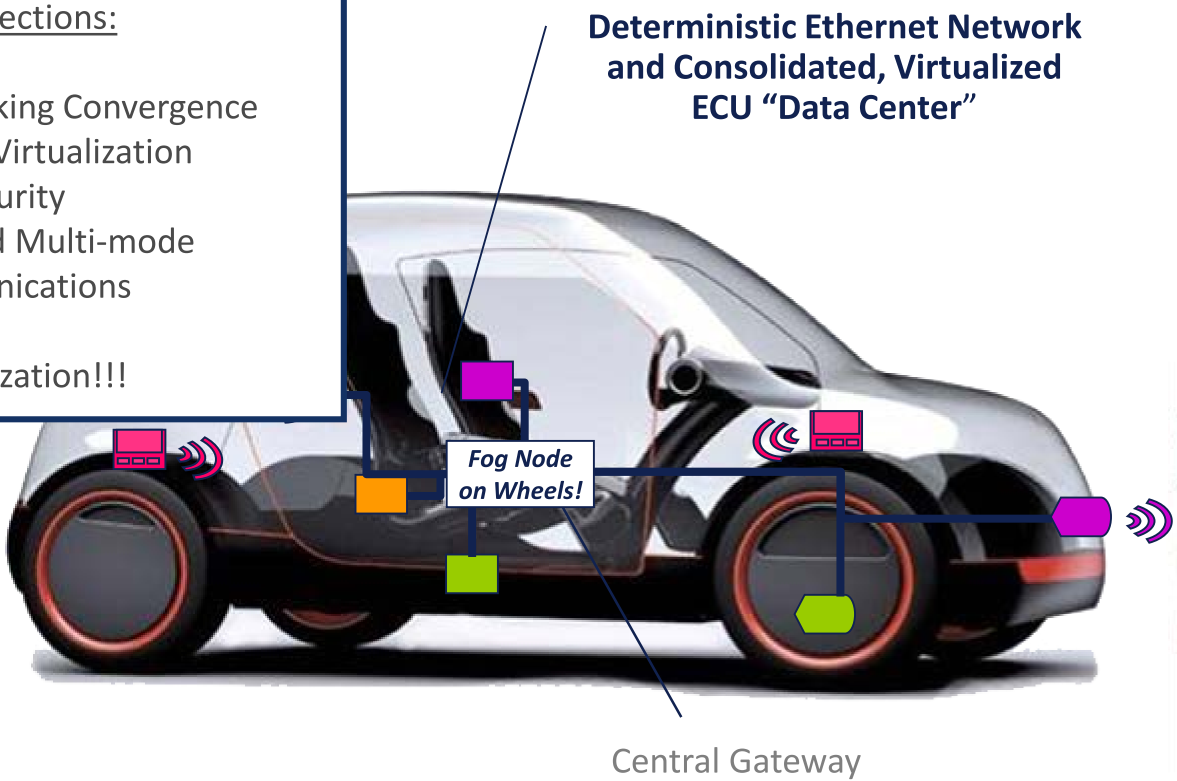
The Role of Fog Computing in the Automobile Evolution

The Future Car Domain Controller is a Fog Node! (Ricky Hudi, former Audi Head of Electronics)

Key Directions:

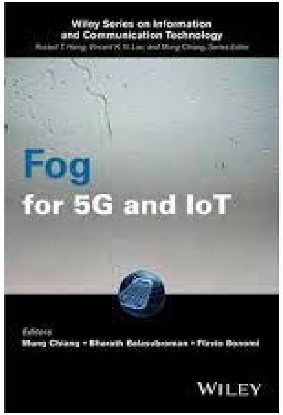
Internal Networking Convergence
Computing Virtualization
Security
Mobility and Multi-mode Communications

Centralization!!!



Deterministic Ethernet Network and Consolidated, Virtualized ECU "Data Center"

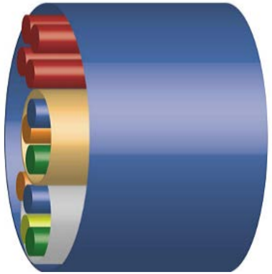
Central Gateway

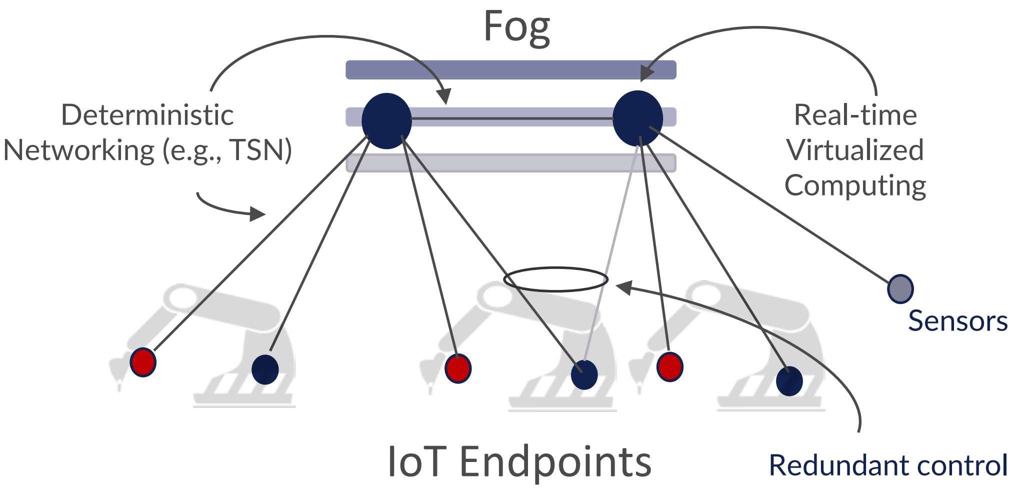

Wiley Series on Information and Communication Technology
Fog
for 5G and IoT
Editors
Mung Chiang • Bharath Balasubramanian • Flavio Bonomi
WILEY

Fog Computing: Enabling the Implementation of Hierarchical, Redundant Control

Deterministic Networking and Real-time Virtualized Computing enable the Convergence of Multiple Control Functions, one step removed from the controlled Endpoints, with separation of Layers of Control

Software Defined Machines!





Fog

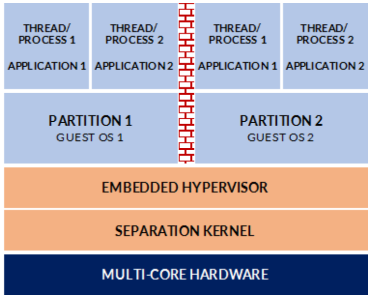
Deterministic Networking (e.g., TSN)

Real-time Virtualized Computing

Sensors

IoT Endpoints

Redundant control



THREAD/ PROCESS 1 APPLICATION 1

THREAD/ PROCESS 2 APPLICATION 2

THREAD/ PROCESS 1 APPLICATION 1

THREAD/ PROCESS 2 APPLICATION 2

PARTITION 1 GUEST OS 1

PARTITION 2 GUEST OS 2

EMBEDDED HYPERVISOR

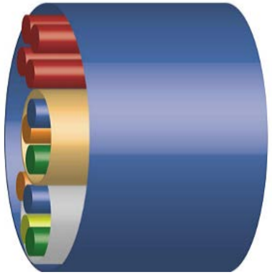
SEPARATION KERNEL

MULTI-CORE HARDWARE

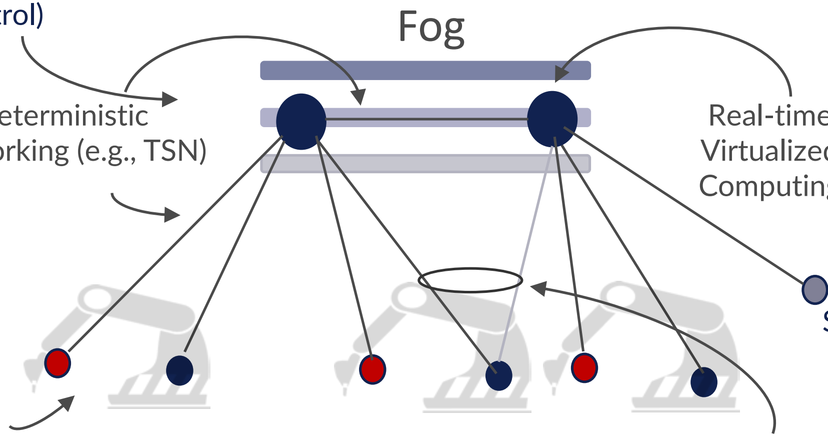
Fog Computing: Enabling the Implementation of Hierarchical, Redundant Control

Deterministic Networking and Real-time Virtualized Computing enable the Convergence of Multiple Control Functions, one step removed from the controlled Endpoints, with separation of Layers of Control

Software Defined Machines!



Higher level control (e.g., logic control)

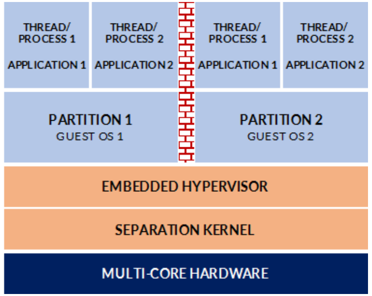

Fog
Deterministic Networking (e.g., TSN)
Real-time Virtualized Computing

Sensors

Low level control (e.g., motion control)

IoT Endpoints

Redundant control

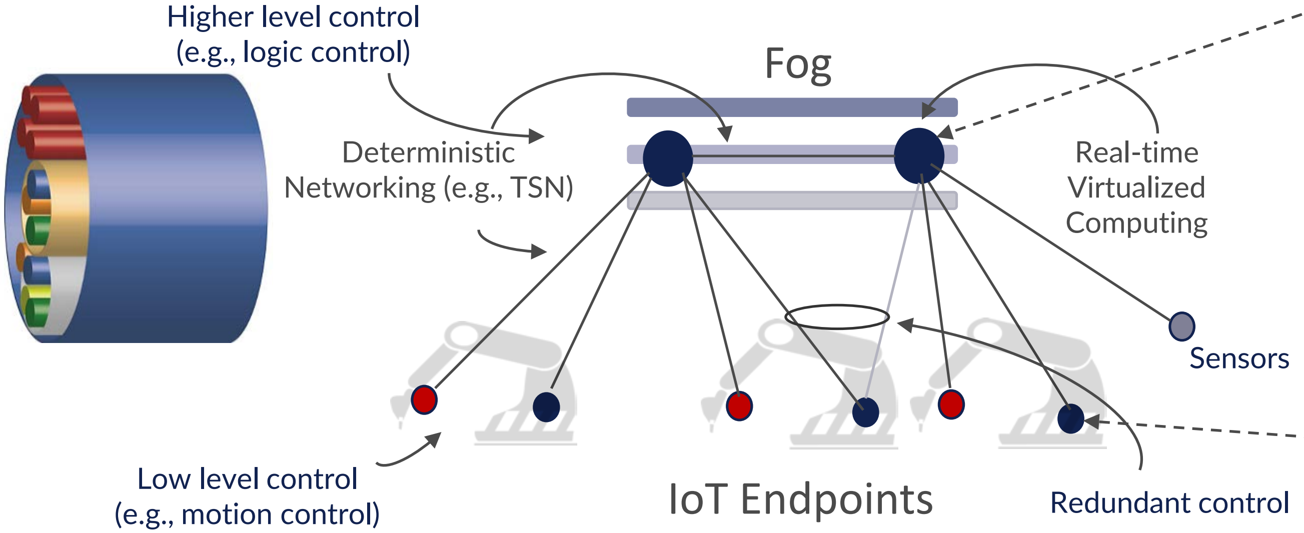


THREAD/ PROCESS 1 APPLICATION 1	THREAD/ PROCESS 2 APPLICATION 2	THREAD/ PROCESS 1 APPLICATION 1	THREAD/ PROCESS 2 APPLICATION 2
PARTITION 1 GUEST OS 1		PARTITION 2 GUEST OS 2	
EMBEDDED HYPERVISOR			
SEPARATION KERNEL			
MULTI-CORE HARDWARE			

Fog Computing: Enabling the Implementation of Hierarchical, Redundant Control

Deterministic Networking and Real-time Virtualized Computing enable the Convergence of Multiple Control Functions, one step removed from the controlled Endpoints, with separation of Layers of Control

Software Defined Machines!



THREAD/ PROCESS 1 APPLICATION 1
THREAD/ PROCESS 2 APPLICATION 2
THREAD/ PROCESS 1 APPLICATION 1
THREAD/ PROCESS 2 APPLICATION 2

PARTITION 1 GUEST OS 1
PARTITION 2 GUEST OS 2

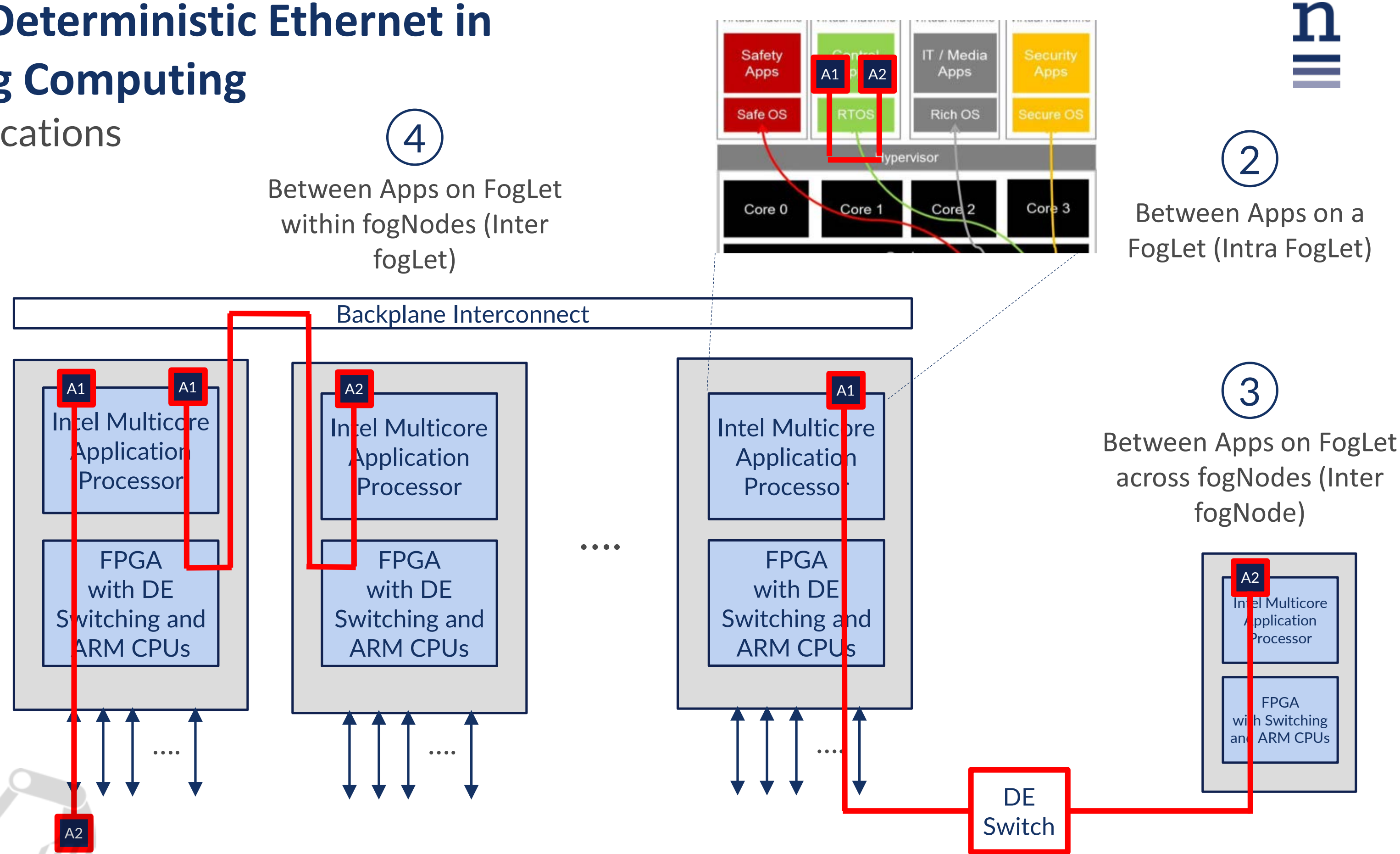
EMBEDDED HYPERVISOR

SEPARATION KERNEL

MULTI-CORE HARDWARE

Key Roles of Deterministic Ethernet in Real-Time Fog Computing

Many Communications Scenarios



1 Between fogNodes and Endpoints (Fieldbus role)

2 Between Apps on a FogLet (Intra FogLet)

3 Between Apps on FogLet across fogNodes (Inter fogNode)

4 Between Apps on FogLet within fogNodes (Inter fogLet)

Deterministic Ethernet

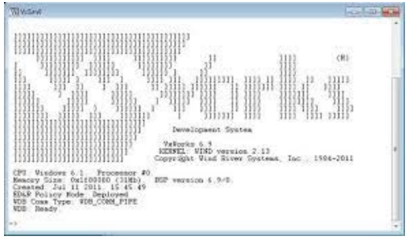
A Real-time App

Fog Computing Requires Deterministic Computing

INTEL® TIME COORDINATED COMPUTING TECHNOLOGY CAN SYNCHRONIZE NETWORKS OF DEVICES TO WITHIN A MICROSECOND.

Critical Building Blocks:

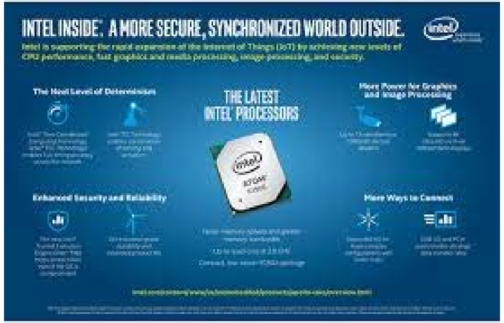
- Microsecond timing distribution
- Synchronized I/O
- Deterministic cache and memory management
- Improved interrupt management
- Deterministic resource scheduling and separation
- Real-time OS and Hypervisors



```
                                                   Development System

                                                 VxWorks 6.9
                                                KERNEL: WIND version 2.13
                                               Copyright Wind River Systems, Inc., 1984-2011

CPU: Windows 6.1.  Processor #0.
Memory Size: 0x1f00000 (31Mb).  BSP version 6.9/0.
Created: Jul 11 2011, 15:45:49
ED&R Policy Mode: Deployed
WDB Comm Type: WDB_COMM_PIPE
WDB: Ready
->
```



INTEL INSIDE®. A MORE SECURE, SYNCHRONIZED WORLD OUTSIDE.

Intel is supporting the rapid expansion of the Internet of Things (IoT) by achieving new levels of CPU performance, fast graphics and media processing, image processing, and security.

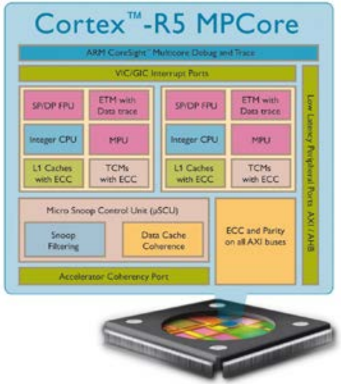
The Next Level of Determinism

THE LATEST INTEL® PROCESSORS

More Power for Graphics and Image Processing

Enhanced Security and Reliability

More Ways to Connect



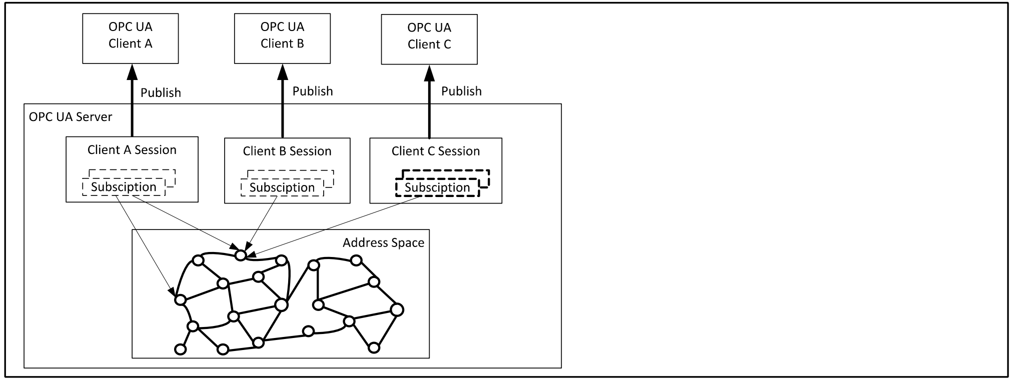
Cortex™-R5 MPCore

QNX™

LYNX SOFTWARE TECHNOLOGIES

Fog Computing Requires Real-time Capable Middleware

- OPC UA over TSN
- DDS
- CubeFog CubeProtocol



OPC UA Client A

OPC UA Client B

OPC UA Client C

Publish

Publish

Publish

OPC UA Server

Client A Session

Subscipton

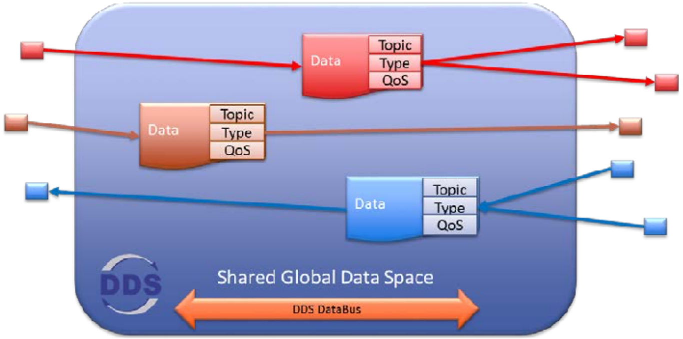
Client B Session

Subscription

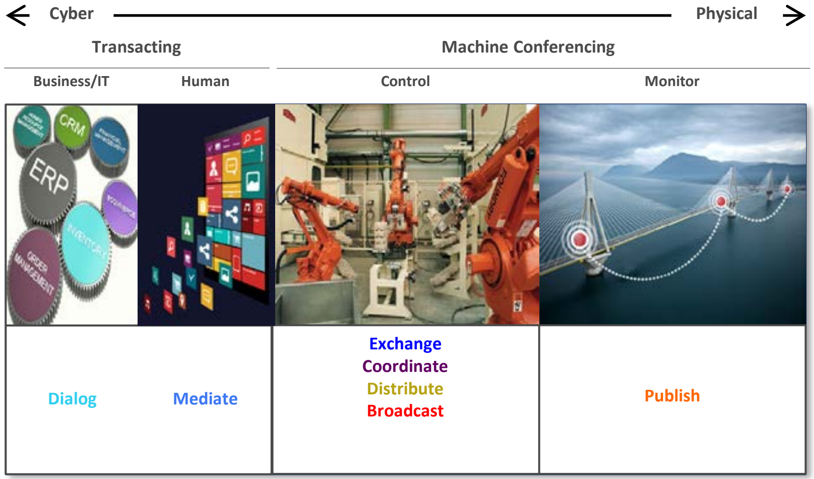
Client C Session

Subscription

Address Space



DDS connects data readers and writers through a virtual concept called the Shared Global Data Space. Each data item has a name (Topic) and a schema (Type). Each dataflow path is independent. Each path is independently controlled by Quality of Service (QoS) settings. There are no servers. Readers and writers interact only through the address space. As a connectivity layer, DDS is much more than a protocol.



Cyber

Physical

Transacting

Machine Conferencing

Business/IT

Human

Control

Monitor

Dialog

Mediate

Exchange
Coordinate
Distribute
Broadcast

Publish