



**OBJECT MANAGEMENT GROUP**

# **OMG IIoT Standards at Work**

## **An Overview**

**Andrew Watson**  
**OMG Technical Director**

# Introducing OMG

- One of the most successful forums for creating open integration standards in the computer industry
  - Middleware platforms (DDS, CORBA & related specs)
  - Modelling platforms (UML, BPMN, SysML & related work)
  - Systems Assurance (SACM, DAF for SSCD ...)
  - Vertical domain specifications (C4I, Robotics, Healthcare ...)
- Member-controlled industrial consortium
  - Both vendors and users
  - Not-for-profit
- Interfaces freely available to all
  - Visit <http://www.omg.org>



# Worldwide Membership



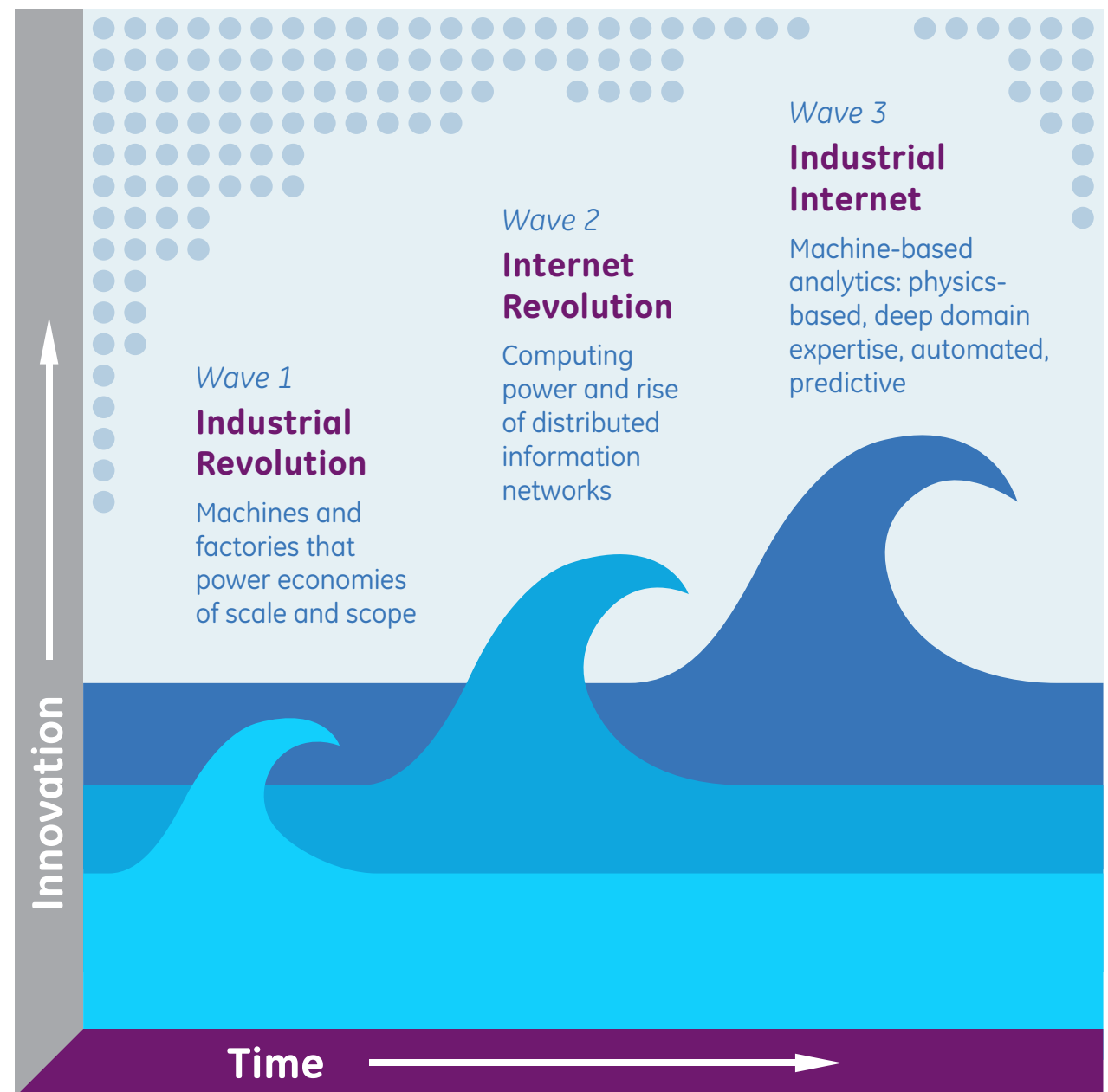
<b>ACORD</b>	<b>EDM Council</b>	<b>Microsoft</b>	<b>OSD</b>	<b>Sparx</b>
<b>Adaptive</b>	<b>EMC</b>	<b>Micro Focus</b>	<b>Penn Nat'l</b>	<b>State St</b>
<b>Adelard LLP</b>	<b>FICO</b>	<b>MID GmbH</b>	<b>PrismTech</b>	<b>Thales</b>
<b>Airbus Grp</b>	<b>FSTC/BITS</b>	<b>MITRE</b>	<b>PROSTEP AG</b>	<b>Thematix</b>
<b>Appian</b>	<b>Fujitsu</b>	<b>Mitsubishi</b>	<b>PTC</b>	<b>TIBCO</b>
<b>AT&amp;T</b>	<b>Gen. Electric</b>	<b>Mphasis</b>	<b>PwC</b>	<b>Toshiba</b>
<b>BAE Systems</b>	<b>HPE</b>	<b>NASA</b>	<b>Remedy IT</b>	<b>Toyota</b>
<b>Bizagi</b>	<b>Honda</b>	<b>NARA</b>	<b>Rolls-Royce</b>	<b>Twin Oaks</b>
<b>Bloomberg</b>	<b>Huawei</b>	<b>NEC</b>	<b>RTI</b>	<b>Unisys</b>
<b>Boeing</b>	<b>IBM</b>	<b>No Magic</b>	<b>SAP</b>	<b>VDMbee</b>
<b>CA</b>	<b>KDM Analytic</b>	<b>Northrop</b>	<b>Selex ES</b>	<b>Visumpoint</b>
<b>Camunda</b>	<b>Lockheed</b>	<b>Oracle</b>	<b>Softeam</b>	<b>WebRatio</b>
<b>Eclipse Fndn.</b>	<b>MEGA</b>	<b>Orbus</b>	<b>Software AG</b>	<b>(200+ more)</b>

# Availability

- **OMG adopts and publishes interface specifications**
  - **Implementation available from at least one OMG member**
- **Interfaces freely available to all (members or not)**
  - **No export restrictions**
  - **No specification licence, no payment**
  - **Best-effort assurances on IPR constraints**
- **Decisions taken by members**
  - **Strategic direction controlled by Board**
  - **Technical direction determined by Technology Committees**
- **Long-term ties to ISO sees many OMG specifications republished unchanged as International Standards**

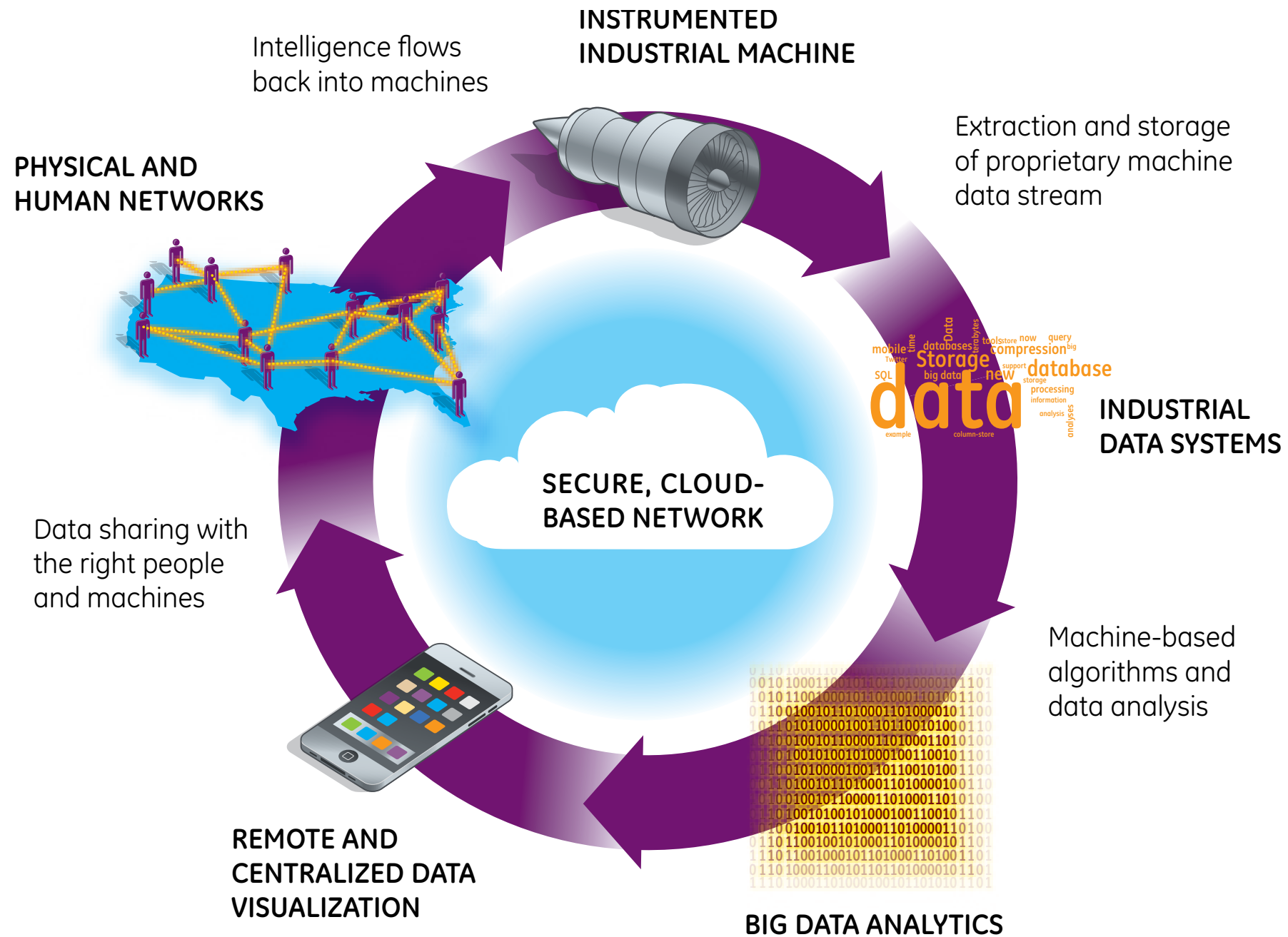
# IIoT: The Next Economic Revolution?

- Industrial revolution replaced muscle power with machines
  - **Dramatic, continuing rise in global living standards began**
- Information revolution similarly boosted brain power
- Their convergence promises further wave of rising productivity and prosperity



Source: Evans & Annunziata, GE, 26 Nov 2012

# Industrial Internet Data Loop



Source: Evans & Annunziata, GE, 26 Nov 2012

# The Benefits

What if... Potential Performance Gains in Key Sectors

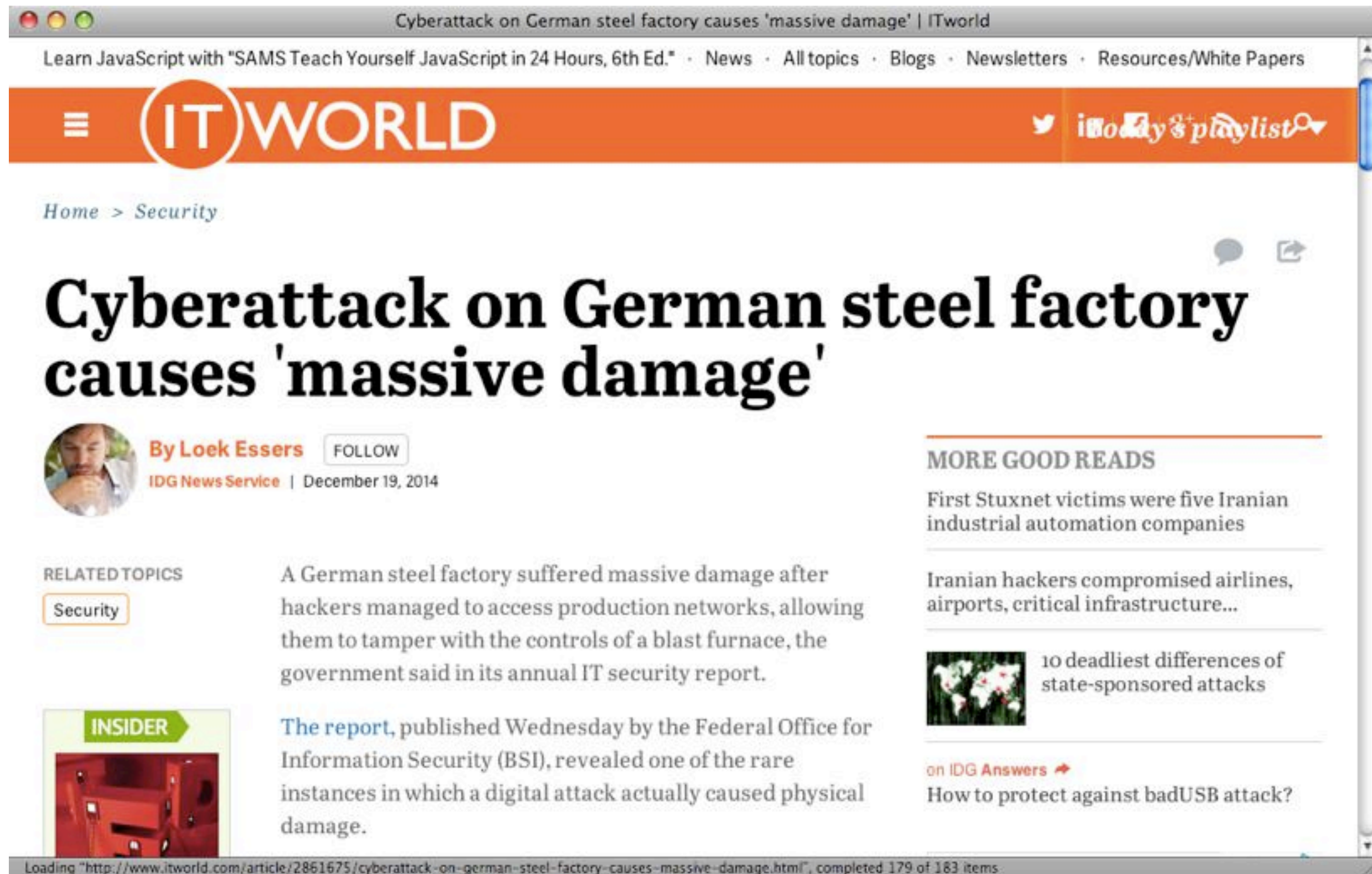
Industry	Segment	Type of Savings	Estimated Value Over 15 Years (Billion nominal US dollars)
Aviation	Commercial	1% Fuel Savings	\$30B
Power	Gas-fired Generation	1% Fuel Savings	\$66B
Healthcare	System-wide	1% Reduction in System Inefficiency	\$63B
Rail	Freight	1% Reduction in System Inefficiency	\$27B
Oil & Gas	Exploration & Development	1% Reduction in Capital Expenditures	\$90B

Note: Illustrative examples based on potential one percent savings applied across specific global industry sectors.  
Source: GE estimates

Source: Evans & Annunziata, GE, 26 Nov 2012



# The Risks



The screenshot shows a web browser window displaying an article on the ITWorld website. The browser's address bar shows the URL: `http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html`. The article title is "Cyberattack on German steel factory causes 'massive damage'", written by Loek Essers for the IDG News Service on December 19, 2014. The article text states that a German steel factory suffered massive damage after hackers accessed production networks, tampering with a blast furnace. A related topic "Security" is highlighted. On the right, there are sections for "MORE GOOD READS" including "First Stuxnet victims were five Iranian industrial automation companies" and "Iranian hackers compromised airlines, airports, critical infrastructure...". A small image of a world map is shown next to the text "10 deadliest differences of state-sponsored attacks". At the bottom, there is a link to "on IDG Answers" with the title "How to protect against badUSB attack?". The browser's status bar at the bottom indicates "Loading 'http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html', completed 179 of 183 items."

Cyberattack on German steel factory causes 'massive damage' | ITworld

Learn JavaScript with "SAMS Teach Yourself JavaScript in 24 Hours, 6th Ed." · News · All topics · Blogs · Newsletters · Resources/White Papers

ITWORLD

Home > Security

## Cyberattack on German steel factory causes 'massive damage'

By Loek Essers [FOLLOW](#)

IDG News Service | December 19, 2014

RELATED TOPICS

Security

INSIDER

A German steel factory suffered massive damage after hackers managed to access production networks, allowing them to tamper with the controls of a blast furnace, the government said in its annual IT security report.

The report, published Wednesday by the Federal Office for Information Security (BSI), revealed one of the rare instances in which a digital attack actually caused physical damage.

MORE GOOD READS

First Stuxnet victims were five Iranian industrial automation companies

Iranian hackers compromised airlines, airports, critical infrastructure...

10 deadliest differences of state-sponsored attacks

on IDG Answers →

How to protect against badUSB attack?

Loading "http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html", completed 179 of 183 items

Copyright © 2015 IDG Enterprise. All rights reserved.





The screenshot shows a web browser window with the title "4.5 million routers hacked in Brazil - Infosecurity Magazine". The browser's address bar shows "4.5 million routers hacked in Br...". The Infosecurity Magazine logo is visible in the top right corner of the page, with the tagline "STRATEGY | INSIGHT | TECHNOLOGY". The article's breadcrumb trail reads "INFOSECURITY MAGAZINE HOME » NEWS » 4.5 MILLION ROUTERS HACKED IN BRAZIL". The article is dated "2 OCT 2012" and is categorized as "NEWS". The main headline is "4.5 million routers hacked in Brazil". Below the headline is a photograph of a network switch with ports labeled "DSL" and "INTERNET". To the left of the main text, a text box states: "Some 300,000 modems in Brazil are still thought to be controlled by attackers". The main text of the article begins: "The forensic breakdown of the attack came first from Fabio Assolini, a researcher for Kaspersky Labs, during a presentation at the Virus Bulletin conference. Graham Cluley at Sophos recounted the presentation in his blog." The second paragraph continues: "Assolini described how at some Brazilian ISPs, more than 50% of users were reported to have been affected by the attack. After the six manufacturers affected issued firmware updates to plug the security hole, the number of compromised modems decreased. However, some 300,000 modems are still thought to be controlled by attackers."

Copyright © 2015 Reed Exhibitions Ltd.

## IIoT prerequisites include ...

- Sensors & advanced instrumentation embedded in machines of all types, collecting data & providing fine-grained control
  - Enormous data volumes distributed & analysed in real time
- Unparalleled cyber security to protect sensitive information
  - Stop bad actors remotely interfering in physical systems
- Designers with tools & skills cutting across multiple engineering disciplines, data science, cyber security, UIs
  - Squeezing inefficiencies out of complex systems
- OMG publishes widely-used specifications in all these areas
  - Already enabling IIoT-based innovation
  - Some relevant OMG activities are ...

# SysML

- Graphical modelling language for specifying, analyzing, designing & verifying complex systems that may include hardware, software, information, personnel, procedures
  - Provides means to precisely model large, complex systems-of-systems, from requirements to acceptance
- Aids communication across engineering disciplines
  - Co-developed with International Council on Systems Engineering (INCOSE)
  - Widespread tool support
  - Mature, widely-used



# Interaction Flow Modelling Language (IFML)

- **User interface design will make or break IIoT systems**
  - Much IIoT debate centres on machine/machine interactions
  - ... but data visualisation & analysis put humans in the loop
  - Seamless interaction with hardware & software to minimise unnecessary input & undesired output is essential
- **IFML describes user's interaction with system**
  - Independent of presentation technology
  - Focussed on structure of user interactions
  - No definition of graphics or styles



# Assurance

- **Measure of confidence that system meets policy goals**
- **Information Assurance (IA)**
  - **Availability, integrity, confidentiality, non-repudiation**
- **Safety Assurance (SfA)**
  - **Risk to the safety of people & equipment**
- **Software Assurance (SwA)**
  - **Free of exploitable vulnerabilities, functions to specification**
- **System Assurance (SysA)**
  - **All applicable safety, security, reliability, regulatory etc goals are met**

# OMG Systems Assurance specifications

- **Common framework for analysis & exchange of information about system assurance and trustworthiness, including ...**
- **Structured Assurance Case Metamodel**
  - **For representing auditable claims, arguments & evidence that system satisfies particular requirements**
- **Automated Source Code Security Measure**
  - **Measured by detecting most-exploited source-code weaknesses (e.g. SQL Injection 1st, Buffer overflow 3rd)**
- **Dependability Assurance Framework for Safety-Sensitive Consumer Devices**
  - **Methodology for dependability argumentation for safety-sensitive consumer devices with embedded software**



## Data Distribution Service

- Integration “glue” for IIoT applications spanning data centres to edge sensors
  - Creates virtual, decentralised global data space abstraction
  - Excellent performance with real-time guarantees
  - Proven-interoperable products from multiple vendors
  - Available for safety-critical systems to DO-178C Level A
  - Integrated security framework
  - Fine-grained access control
  - Highly scalable
  - Proven in multiple mission-critical applications





**DDS controls Grand Coulee Dam**

**Largest US hydro-electric plant  
(6.8 GW)**

**Fastest-responding major power  
source on Western Grid**



A photograph of the NASA Orion rocket on the Mobile Launcher Platform (MLP) being moved by the Orbital Launch System (OLS) crawler-transporter. The MLP consists of three yellow and white boosters. The Orion service module is mounted on top of the central booster. The MLP is being transported on a set of concrete blocks. The background shows the launch complex structure and a large crane.

**Kennedy Space  
Centre**

**NASA Orion  
Launch Control  
System**

**First Launch  
5 Dec 2014**

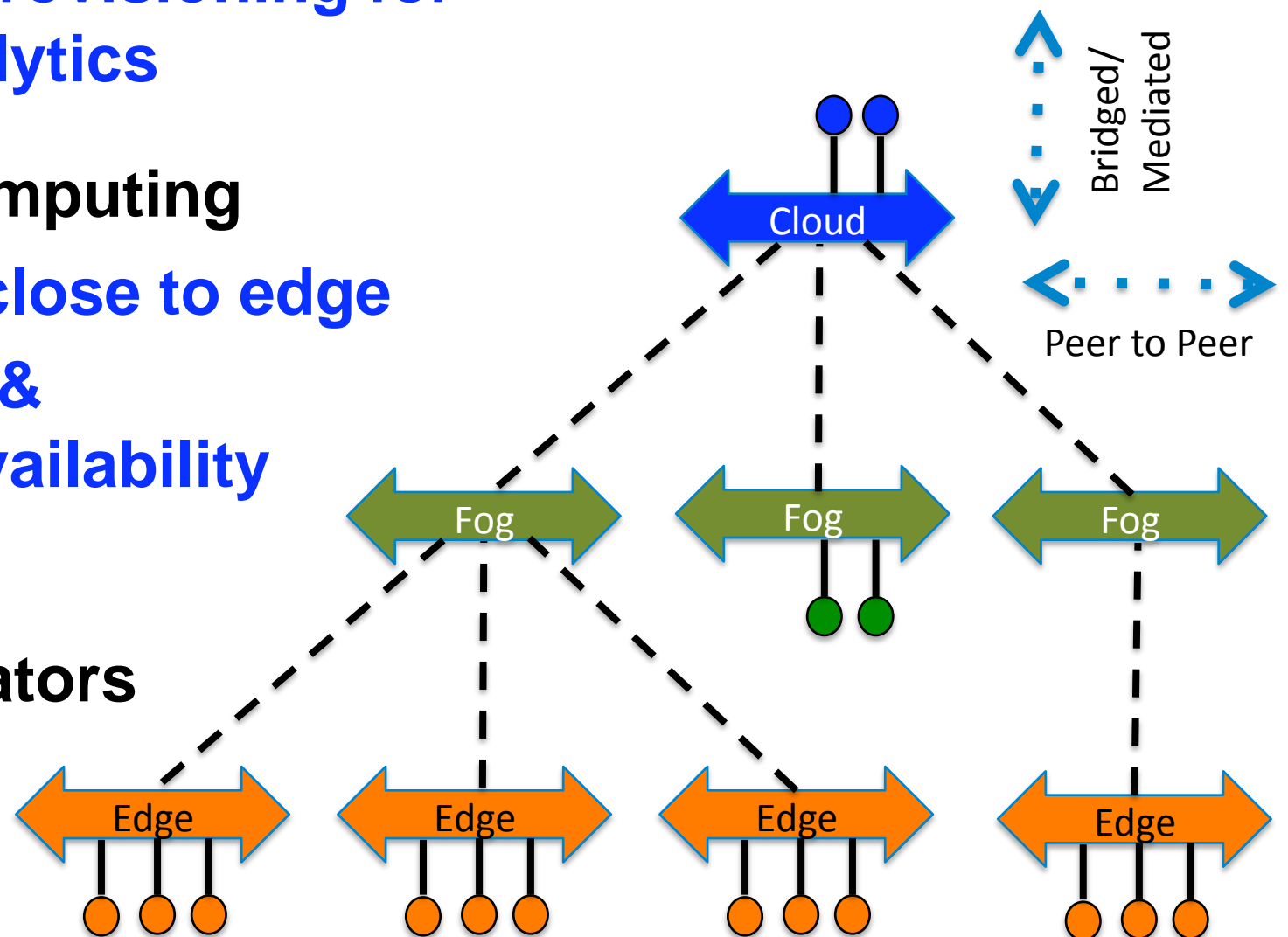
**DDS-based  
SCADA system**

**400k msgs/sec**



# DDS from Edge to Fog to Cloud

- **“Cloud” Data Centres**
  - Elasticity, flexible provisioning for Management & analytics
- **“Fog” Distributed Computing**
  - Process bulk data close to edge
  - Reduce bandwidth & latency, increase availability & robustness
- **“Edge” sensors/actuators**
  - High-volume data sources, realtime actuators

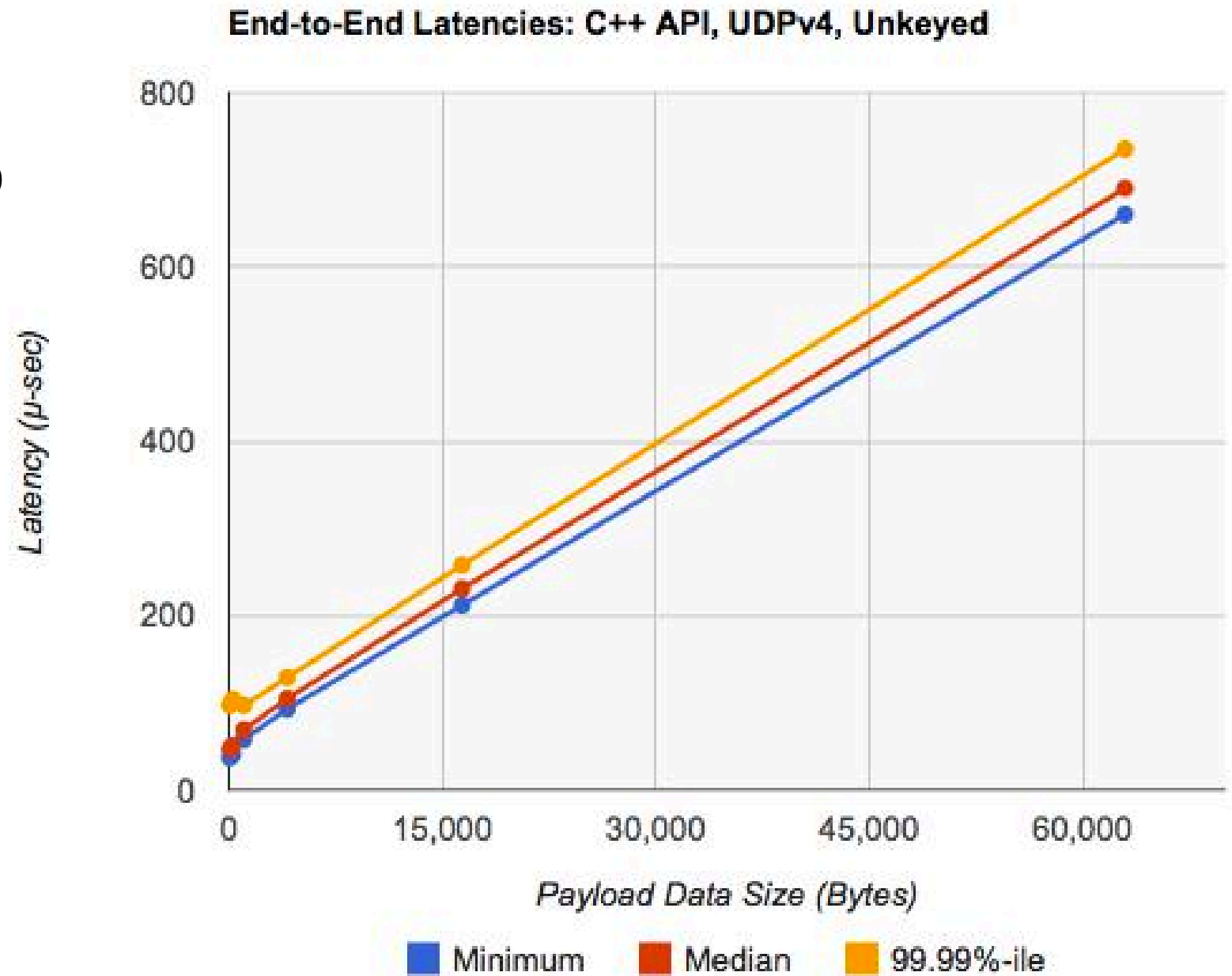


# DDS Wire Protocol Optimised for IIoT

- **Peer-to-peer:** no brokers or servers, no single point of failure
- **Adaptable QoS:** multiple policies, including prioritization
- **Reliable:** even over multicast!
- **Any size data:** automatic fragmentation
- **Automatic Discovery:** presence without configuration
- **Decoupled execution:** start/stop apps in any order
- **Efficient data encoding & encapsulation**
- **High performance:** near-native “wire” speeds
- **Linear scalability:** no  $N^2$  network connections

# High performance, highly predictable

- Intel Core2 Quad CPU Q6600
  - 2.4 GHz, 4MB Cache
  - 4GB memory
- Intel Pro 1000 Gigabit Ethernet NIC
  - e1000e chipset
- Link DXS-3350 SR switch
  - 176Gbps Capacity
  - 48 x 10/100/1000BASE-T ports





# Summary: What IoT standards do we need?

- Obviously, for networking together IoT devices
  - To allow multiple vendors' products to work together with minimum (re-)configuration
  - **OMG Data Distribution Service (DDS) fits the bill**
- *In Addition* we need tools, training & (yes) standards for:
  - Specifying, analysing, designing, verifying complex systems
  - Dependability Assurance
  - Threat & risk modelling
  - Measuring Source Code security/robustness
  - ... other Safety, Security & Resilience issues
- **OMG has established standards in all these areas**



## For more information

**OMG:** <http://www.omg.org>

**Email:** [andrew@omg.org](mailto:andrew@omg.org)

**Thank You!**  
**Questions?**