IIoT standards at work

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**

Putting IoT to Work™

Worldwide Membership

|				
ACORD	Eclipse Fndn.	MEGA	OSD	Sparx
Adaptive	EDM Council	Microsoft	PTC	State St
Adelard LLP	EMC	Micro Focus	PrismTech	Thales
Airbus Grp	FICO	Microsoft	PROSTEP AG	Thematix
Appian	FSTC/BITS	MID GmbH	PTC	TIBCO
AT&T	Fujitsu	MITRE	PwC	Toshiba
BAE Systems	Gen. Electric	Mitsubishi	Remedy IT	Toyota
Bizagi	HPe	NASA	Rolls-Royce	Twin Oaks
Bloomberg	Honda	NARA	RTI	Unisys
Boeing	Huawei	NEC	SAP	VDMbee
CA	IBM	No Magic	Selex ES	Visumpoint
Camunda	KDM Analytic	Northrop	Softeam	WebRatio
cébé ITKM	Lockheed	Oracle	Software AG	(200+ more)

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
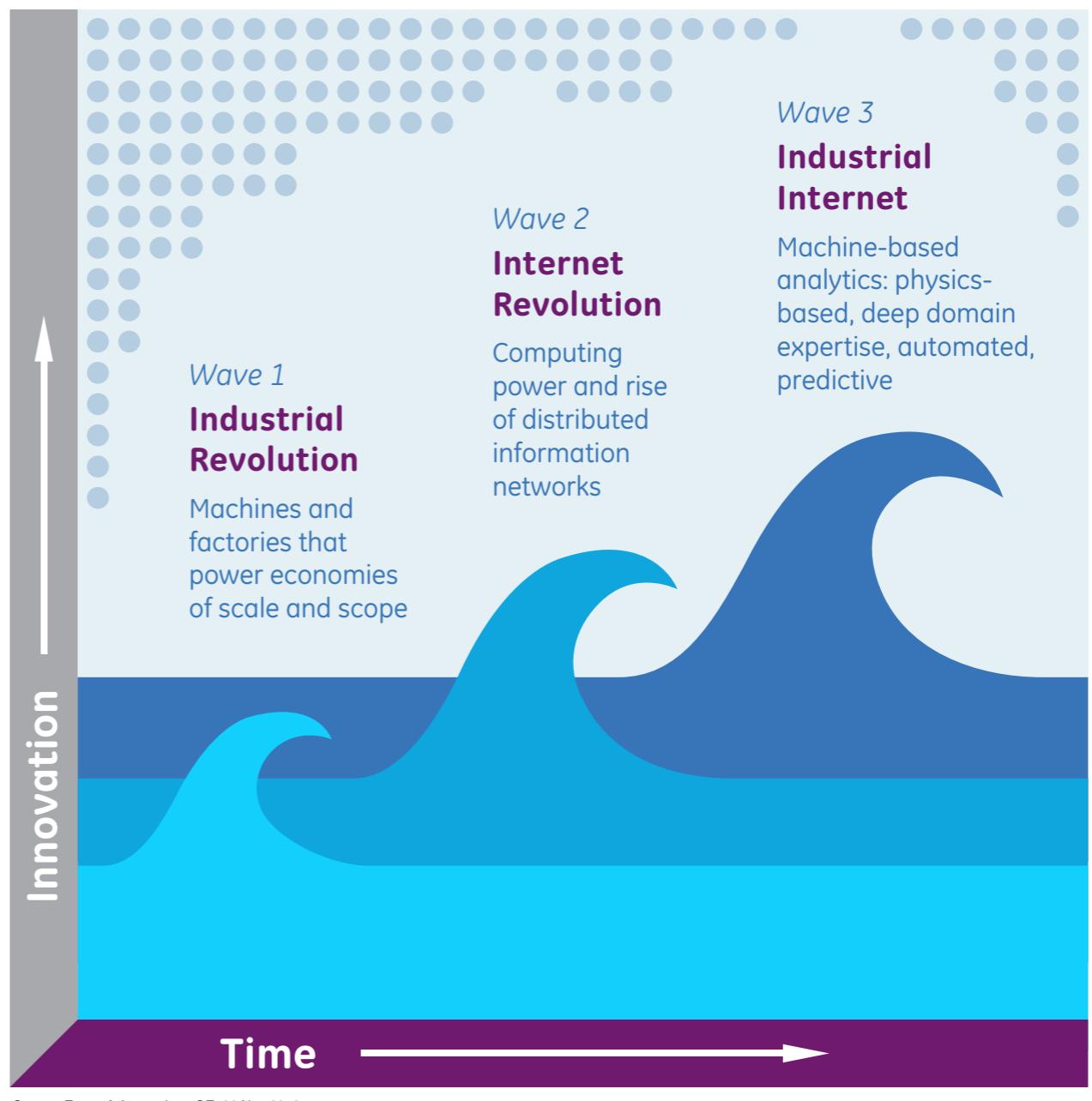
Industrial Internet Data Loop

INSTRUMENTED INDUSTRIAL MACHINE

Intelligence flows back into machines

Extraction and storage of proprietary machine data stream

PHYSICAL AND HUMAN NETWORKS

INDUSTRIAL DATA SYSTEMS

SECURE, CLOUD-BASED NETWORK

Data sharing with the right people and machines

Machine-based algorithms and data analysis

REMOTE AND CENTRALIZED DATA VISUALIZATION

BIG DATA ANALYTICS

Source: Evans & Annunziata, GE, 26 Nov 2012

Putting IoT to Work™

5
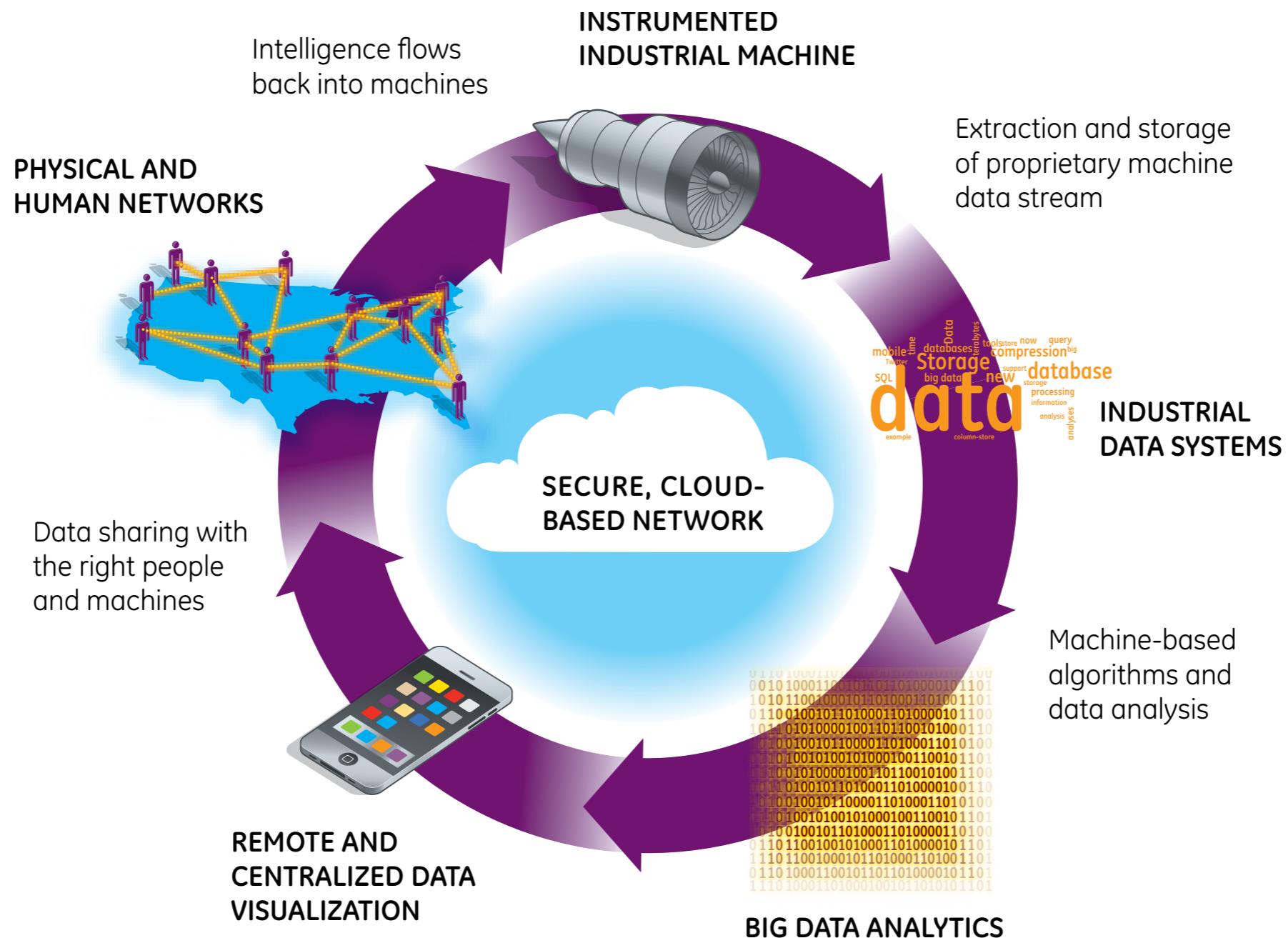
The Numbers

- **GPS-guided John Deere tractors seed fields with no overlaps or gaps between traverses**
  - **10% cost saving = $50/acre (€150/hectare) for cereal farmer**

- **GPS-guided John Deere harvesters runs continuously at optimum 7 kph all day, not human operator's typical 5 kph**
  - **Harvests 30% more in a day, optimising equipment use & weather windows, reducing operator fatigue**

- **Volvo excavators programmed with CAD model of hole to dig**
  - **10-20% faster than human operator**

- **ASDA lorries' deliveries planned & tracked via GPS**
  - **5-10% cost savings, precise prediction of delivery times**

The Risks

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID
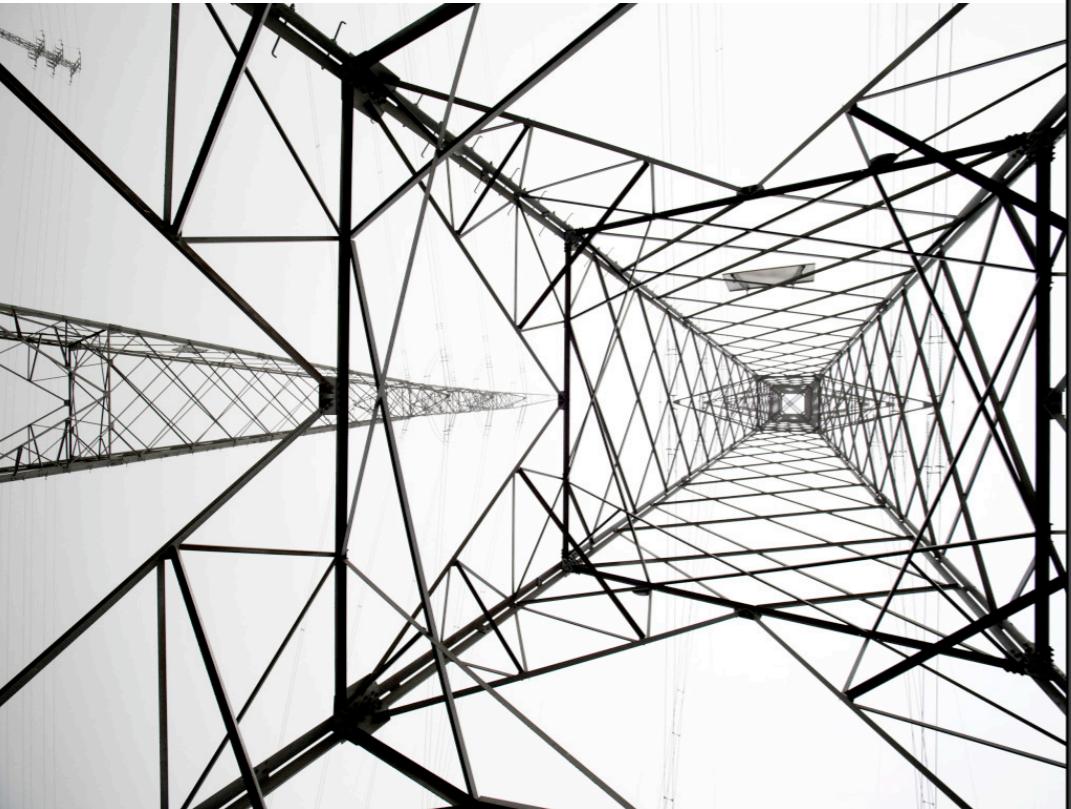
JOSE A. BERNAT BACET/GETTY IMAGES

IT WAS 3:30 p.m. last December 23, and residents of the Ivano-Frankivsk region of Western Ukraine were preparing to end their workday and head home through the cold winter streets. Inside the Prykarpattyaoblenergo

How hackers attacked Ukraine's power grid: Implications for Industrial IoT security

The December 2015 cyberattacks on Ukranian power utilities were rare in that actual damage was inflicted. But there's ample evidence of widespread infiltration into organisations' operational systems.

By Charles McLellan | March 4, 2016 -- 12:54 GMT (12:54 GMT) | Topic: Internet of Things: The Security Challenge

The former Soviet republic of Ukraine has been a trouble-spot since early 2014, which saw the 'Euromaidan' revolution in support of closer EU integration, the Russian annexation of Crimea and the start of the ongoing pro-Russian separatist insurgency.

To add to their woes, large sections of the Ukrainian population suffered power cuts over Christmas 2015 following a series of cyberattacks on three local energy companies. Although widely suspected to be from Russia, the identity of the hackers remains unclear as attribution (https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html) in these matters is complex.

Power plant Burshtyn TES, Ukraine.

Image: Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons)

Ukrainian attack

- **Coordinated attack on 3 regional Ukrainian power companies**
  - **230,000 customers cut off from 1530 to 1830 on 23 Dec 2015**
  - **At least 27 substations taken off-line**

- ***Spear-Phishing* on office IT systems began > 6 mo. previously**
  - **BlackEnergy 3 infection via Word/Excel email attachments**
  - **Keystroke loggers installed to steal logins for ICS networks**

- **Breakers opened using remote PC control software**
  - **Control PCs then crippled using KillDisk (destroys MBR)**
  - **Serial/ethernet bridges sabotaged using custom firmware**
  - **Control Centre UPSs shut down**
  - **Telephone DoS attack against customer call centre**

Putting IoT to Work™ 8

3 Most Important IIoT Design Policy goals

- **Safety**
  - **Does not cause physical injury or damage to health (either directly, or via damage to property & the environment)**

- **Security**
  - **No unintended or unauthorised access, change or destruction of system or data & information it contains**

- **Resilience**
  - **System avoids, absorbs & manages dynamic adversarial conditions while completing assigned mission(s), reconstitutes operational capabilities after casualties**

Source: Industrial Internet Reference Architecture
http://www.iiconsortium.org/IIRA.htm

Demanding requirements

- **Safe, secure & resilient systems**
  - **Documenting & then achieving all design goals, even in the face of bad actors attempting remote interference**

- **Designers who have tools & skills that cut across multiple engineering disciplines, data science, cyber security, UIs**
  - **Squeezing inefficiencies out of complex systems**

- **Sensors & advanced instrumentation embedded in machines**
  - **Enormous data volumes distributed & analysed in real time**

- **Widely-used standards support all these**
  - ***Already* enabling IIoT-based innovation**
  - **Some relevant OMG activities ...**

Putting IoT to Work™

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**

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**

Ontology Definition Metamodel

- **IIoT systems could generate huge amounts of data**

  - **New data categories may be added as systems evolve ...**

  - **... with new units, meanings & relationships to each other**

  - **Hard-wiring static assumptions about data being created, analysed and used would limiting system adaptability**

- **Ontology Definition Metamodel (ODM) provides tools to categorise data & represent complex, evolving relationships**

  - **Enables reasoning about data types & relationships not foreseen at design time**

  - **A vital foundation for data analytics**

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**
  - **Must achieve seamless man-machine interface that minimises unnecessary input & undesired output**

- **IFML supports abstract design of user's interaction with system**
  - **Independent of presentation technology**
  - **Focussed on structure of user interactions**
  - **No definition of graphics or styles**

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™

**DDS controls largest
US hydro-electric plant
(6.8 GW)**

**Fastest-responding major power
source on US Western Grid**
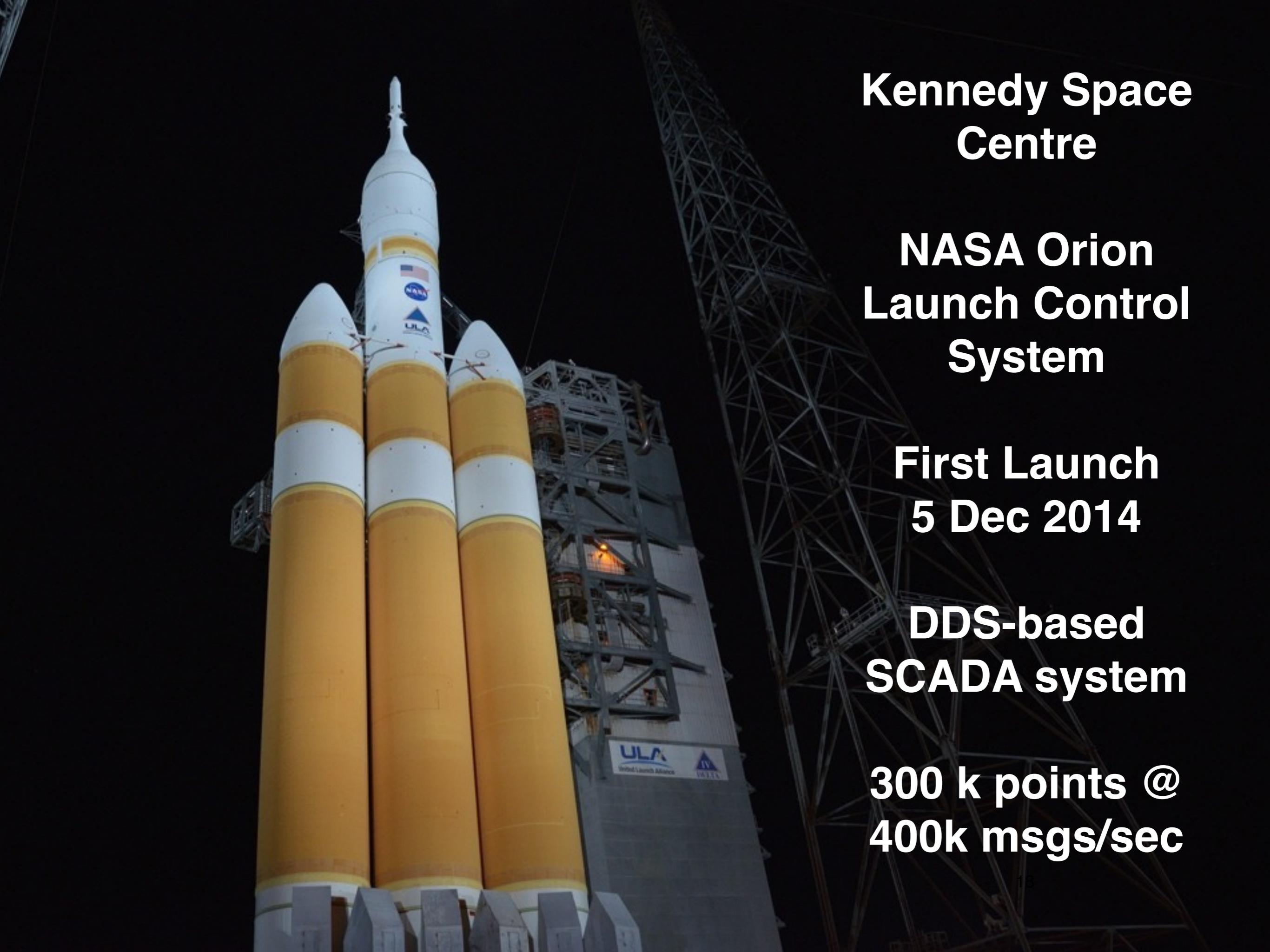
Kennedy Space Centre

NASA Orion Launch Control System

First Launch 5 Dec 2014

DDS-based SCADA system

300 k points @ 400k msgs/sec

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**

- ***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**

- **(And by the way, OMG publishes standards in all these areas)**

For more information

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

Email: **andrew@omg.org**

Thank You!

Questions?