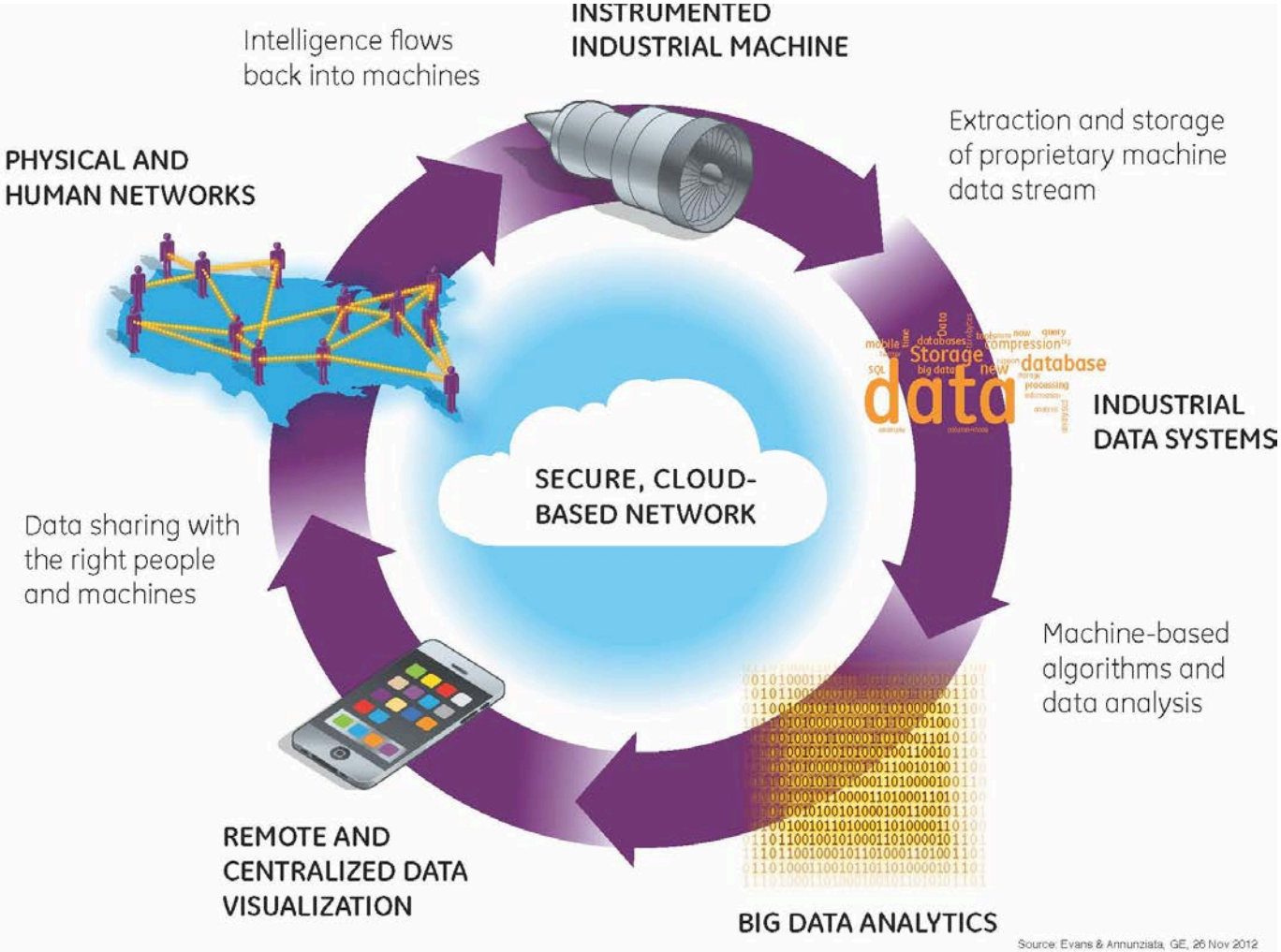
OBJECT MANAGEMENT GROUP

Manufacturing & the Internet of Things

Larry L. Johnson

OMG Technical Director

Industrial Internet Data Loop



3 Most Important IoT Design Policy goals

- Safety
  - Does not cause physical injury or damage to health (eitherdirectly, or via damage to property & the environment)
- Security
  - No unintended or unauthorised access, change ordestruction 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 theface 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 & analyzed in real time
- Widely-used standards support all these
  - Already enabling IIoT-based innovation
  - Some relevant OMG activities ...

OMG Standards Supporting IoT

- SysML
  - Graphical modeling language for specifying, analyzing, designing & verifying complex systems (hardware, software, information, personnel, procedures…)
- Data Distribution Service (DDS)
  - Enables virtual, decentralized global data space abstraction
  - Real-time guarantees, Effective QoS management, Scalable
  - Available for safety-critical systems to DO-178C Level A
- Ontology Definition Metamodel (ODM)
  - Facilitates evolution of meanings & relationships obviating the need for restrictive hardwiring
- Interaction Flow Modelling Language (IFML)
  - Facilitates seamless man-machine interaction
  - Focused on structure of user interactions

IoT Benefits for Manufacturing

- “Agnostic” communication network with gateways to talk to the various controllers using an overall model of the system of systems.
- Analytics layers
  - Six Sigma & other quality analysis using data connected in real-time
  - Big Data – correlate with things that are not obviously connected (such as unsuspected affects of front-end variation on back-end yields)

The Risks

- 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
- Stuxnet
  - Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material.
- U.S. Warns of Hacker Attacks on Energy, Aviation, Manufacturing Industries
  - (Reuters, Jim Finkle, October 23, 2017)
  - The U.S government issued a rare public warning that sophisticated hackers are targeting energy and industrial firms, the latest sign that cyber attacks present an increasing threat to the power industry and other public infrastructure.
  - The Department of Homeland Security and Federal Bureau of Investigation warned in a report distributed by email late on Friday that the nuclear, energy, aviation, water and critical manufacturing industries have been targeted along with government entities in attacks dating back to at least May.

More Risks

- Botnets
  - logical collection of internet-connected devices such computers, smartphones or IoT devices whose security has been breached and control ceded to a third party. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as IRC and Hypertext Transfer Protocol (HTTP)
- Ransomware
  - WannaCry – Encrypted data and demanded ransom payments in the Bitcoin cryptocurrency. Within a day it was reported to have infected more than 230,000 computers in over 150 countries. Parts of the United Kingdom's National Health Service (NHS) were infected, causing it to run some services on an emergency-only basis during the attack. Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide

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 safetysensitive consumer devices with embedded software**

The Hare and the Tortoise

- **Information Technology**
  - **Legendary high-paced evolution**
  - **Increasingly complex systems make threat analysis and identification a daunting task.**
  - **The pace does not exclude Malware which enjoys the surprise of threat discovery**
- **Operational Technology**
  - **Manufacturing machines, networked together.**
  - **Each machine comes with computer and network port... they have lifetimes of 20-30 yrs & generally the controlling/networking software is never upgraded**
  - **There's a lot of networked equipment out there, a mixed bag of age and sophistication with little to no IT control**
  - **It WILL fail due to its ad-hoc inhomogeneous complexity**

Modernization & ReTooling

- Use it or Lose
  - Software built on IoT enabling standards is useless unless it is deployed.
  - We can't just add modern new machines, protocols and architectures to our existing systems and expect any improvement
- I'm Sorry… It's Painful
  - Retrofitting and revamping factory systems requires extensive analysis.
  - Some machines will not be suitably upgradeable and will need replacement

We have much of what we need

- Apply standards-based Assurance tools to discover and minimize Entry Points.
- Carefully monitor each entry point for potential threats.
- Upgrade data transports (DDS)
- Isolation of the factory floor is crucial (subnets or subclouds with reduced entry points)
  - But it can't be total.
  - We're in a distributed world and the human being is still involved.
- Homo Sapiens is one of the most difficult entry points to control… eMail, Social Media, Unscreened Software, Internet Access. (SysML, IFML)

We’re Waking Up

- Companies with “lights-out” factories such as those in the semiconductor industry are scrutinizing their manufacturing systems and undertaking aggressive projects to reduce vulnerabilities.
- It is crucial that we use what we have.

For more information

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

Email: larry@omg.org

Questions?