The Holy Grail of Smart Object Interoperability

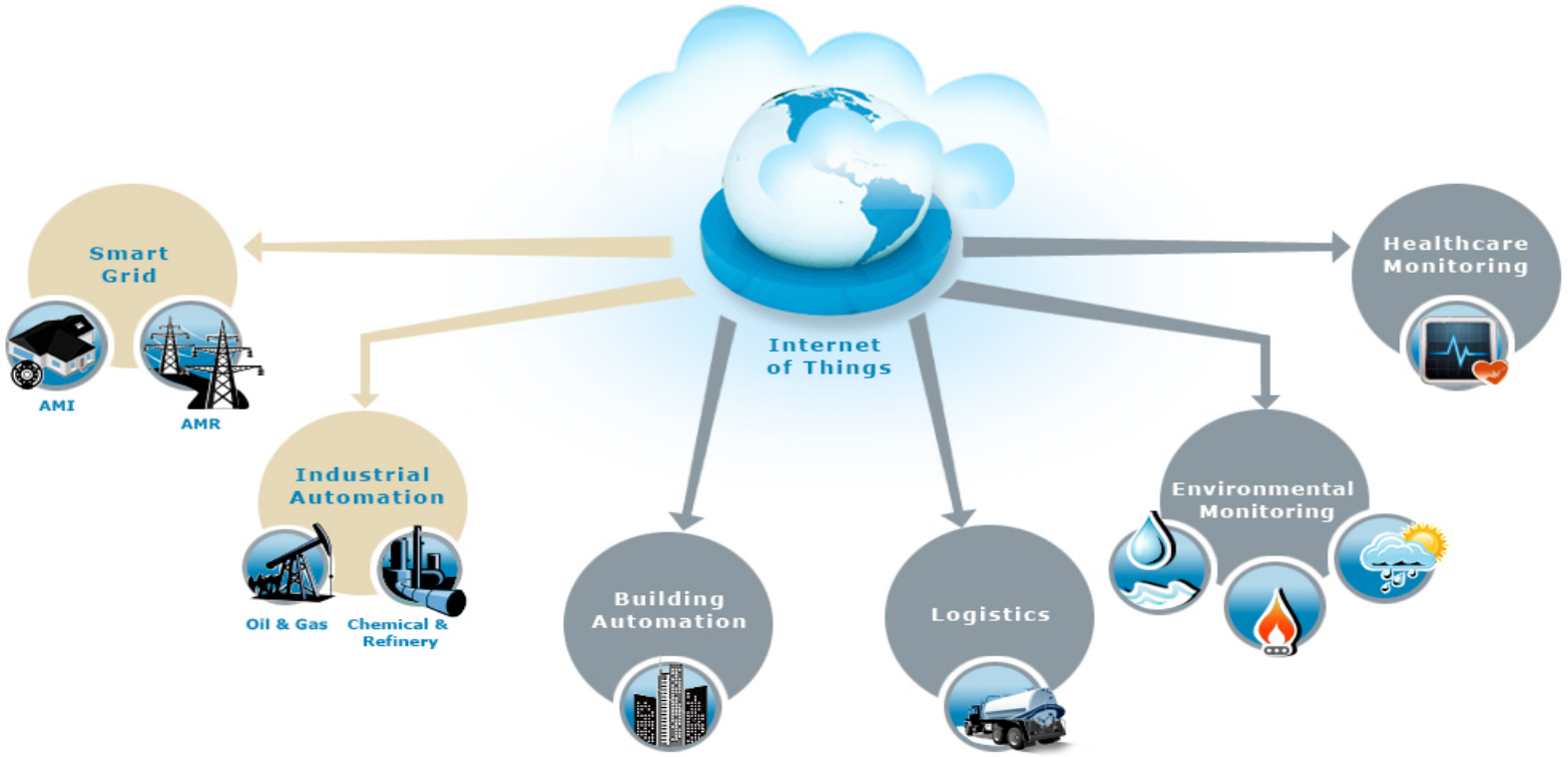
The Process Automation Arena

Robert Assimiti

Many Hands - Even More Gloves

Million $ question: *How do we pave the way towards interoperable and secure connectivity among smart objects in an application and link-layer agnostic manner?*

Current reality: *A wide gamut of standards bodies have tailored application (even niche) and link-layer dependant solutions.*



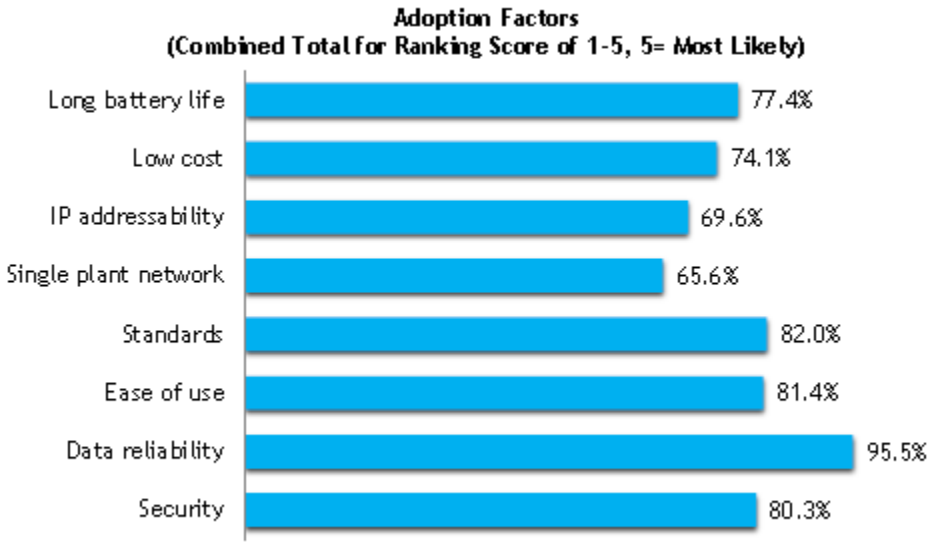
Use Case: Smart Objects in the Process Automation Arena

OnWorld conducted polls and published results based on interviews with 105 plant managers, process integrators and system engineers

Results are clearly indicative of industrial end user's concerns

IPv6 addressability and **standards compliance** are major factors for adoption of smart objects employed in process and factory automation

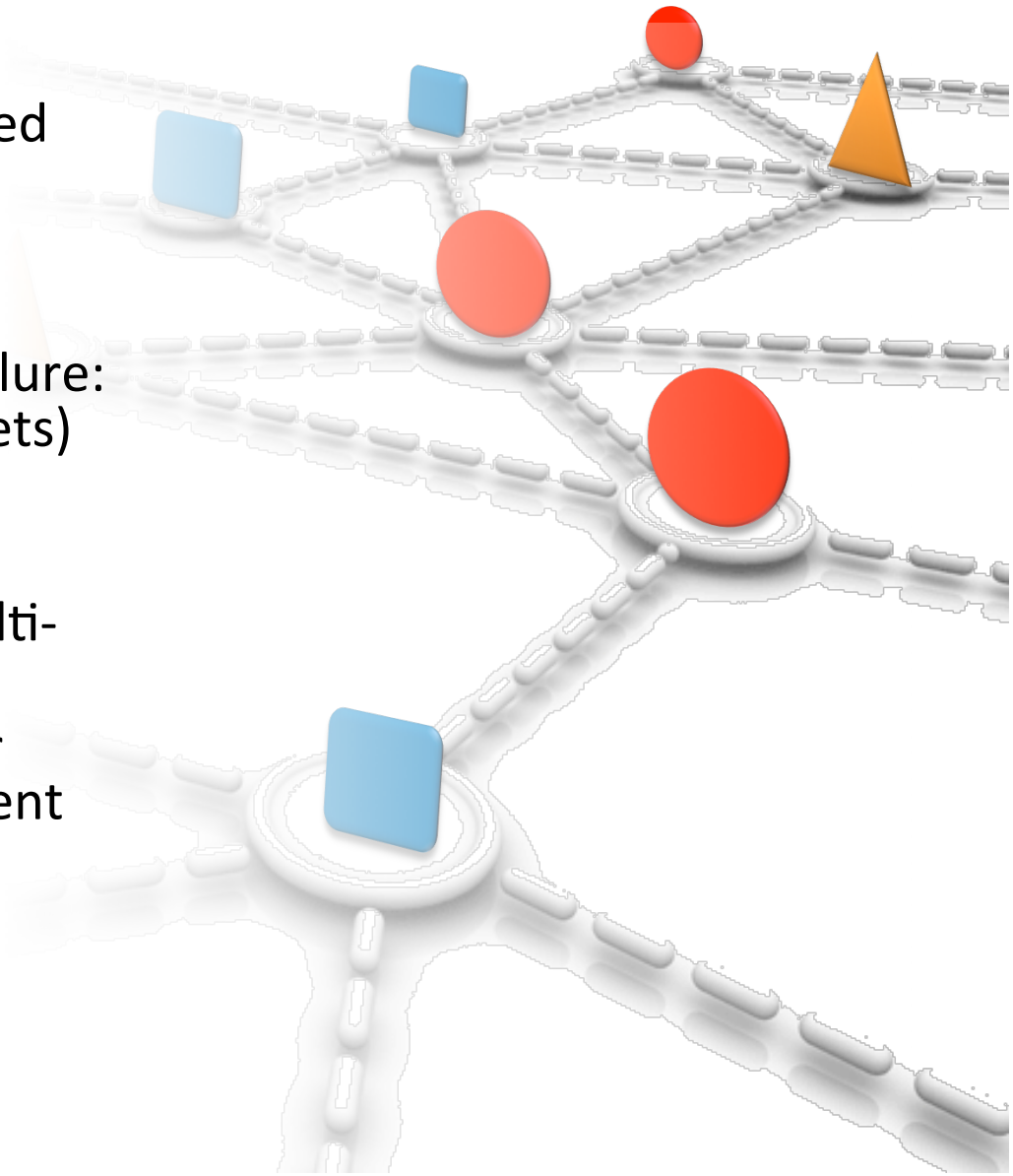
IPv6 compliance is tightly coupled with future extensibility of smart objects based products



Source: "Industrial Wireless Sensor Networks," ON World March 2010

Industrial Smart Object Networks

- Fully deterministic and centralized networks
- Scalability in the hundreds
- Extremely high reliability -> dire consequences associated with failure: 99.9999999% (even in wireless nets)
- Path diversity a must
- Must meet strict guaranteed latencies: sub-second even in multi-hop wireless networks
- Relies heavily on push model for periodic data collection: as frequent as every 100 ms)
- Support for P2P control loops
- Long battery life: 5 -10 years



The Current Global Trifecta

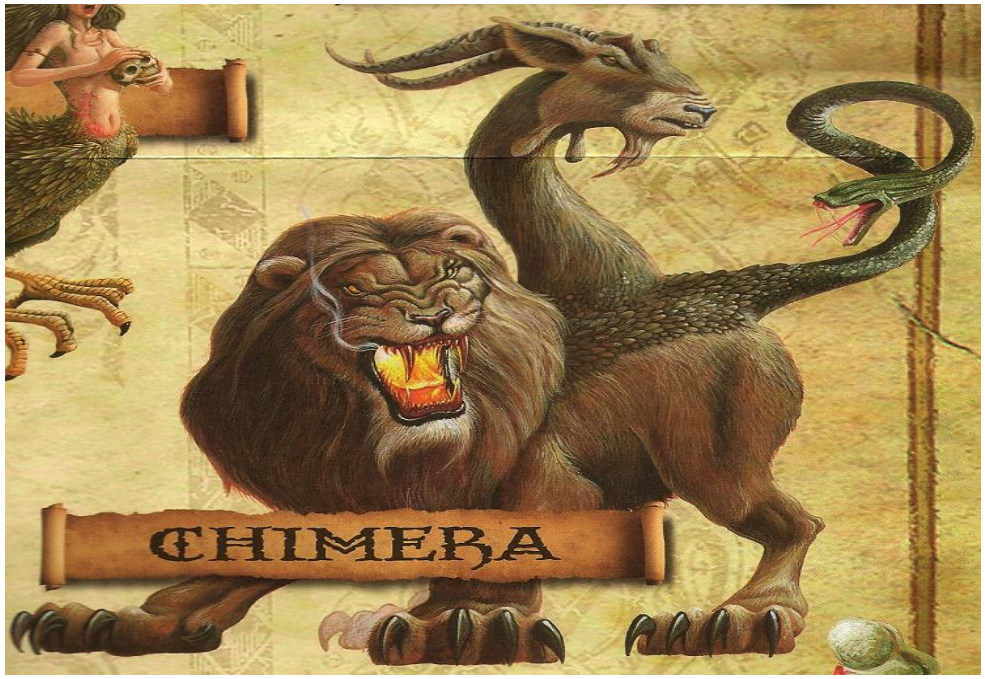
Standard specific means lack of alignment with IETF existing and vetted standards. Standard specific dominates the map at this point. That is so 20th century!!!

Standard	ISA100.11a	Wireless HART	WIA-PA
Networking	IPv6/6loWPAN	Standard specific	Standard specific
Transport	UDP	Standard specific	Standard specific
Routing	Mesh-under but RPL not precluded	Mesh-under	Mesh-under
Web services	None	None	None
Management	Standard specific	Standard specific	Standard specific
Security (end-to-end)	Standard specific at transport layer	Standard specific at application sub-layer	Standard specific at application sub-layer
Provisioning	Standard specific	Standard specific	Standard specific
Backbone networking	IPv6	Standard specific	Standard specific

Smart Objects– The Chimera Threat

Wide gamut of application requirements resulted in deployed networks that exhibit:

- Various degrees of scalability
- Messaging patterns:
  - Bidirectional Client server
  - Push
  - Alerting
- Distributed versus centralized network management paradigms
- "Sleepy" versus "always-on" devices
- Various latency guarantees
- Different security paradigms and policies
- High variability in hardware resources (memory, processing power, etc)



Chimera: "A fire-breathing monster with a lion's head, a goat's body, and a serpent's tail."

THREAT: The smart object ecosystem will end up as a chimera of networking technologies.

The Holy Grail of SO Interoperability

- Holy Grail:
  - No middleboxes/translation gateway
  - Networking and security should be interoperable and independent of application and link layer
- A good starting point:
  - Standardize capability discovery to allow smart objects to learn whether they can interoperate

"You might say that I'm a dreamer, but I'm not the only one."