

Operations Track:

M2M and Mesh Networks

Presented by:

Joseph Andrulis, RF Monolithics

David Shaw, NDS Security

3:10 – 3:50 p.m.

Brady Room

Solutions Approach to M2M Applications

Presented by:

Joe Andrulis

RF Monolithics

RF Monolithics

Established 25 years ago to develop SAW-based component products

Innovator in low power radio throughout its history

- Pioneered automotive RKE systems
- Developed first new radio architecture in over 40 years, the Amplified Sequence Hybrid (ASH) radio
- Shipped over 650,000,000 products into low-power radio applications

Formed the Wireless Systems Group in March 2005 to develop standard and custom low power radio systems for OEM customers

From the outset, WSG advocated a Solutions-Centric approach to M2M problems based on customer needs derived from our real-world experiences

In order to truly solve a customer's problem, all parts of an M2M system must be available and integrated with each other and the customer's existing information systems.

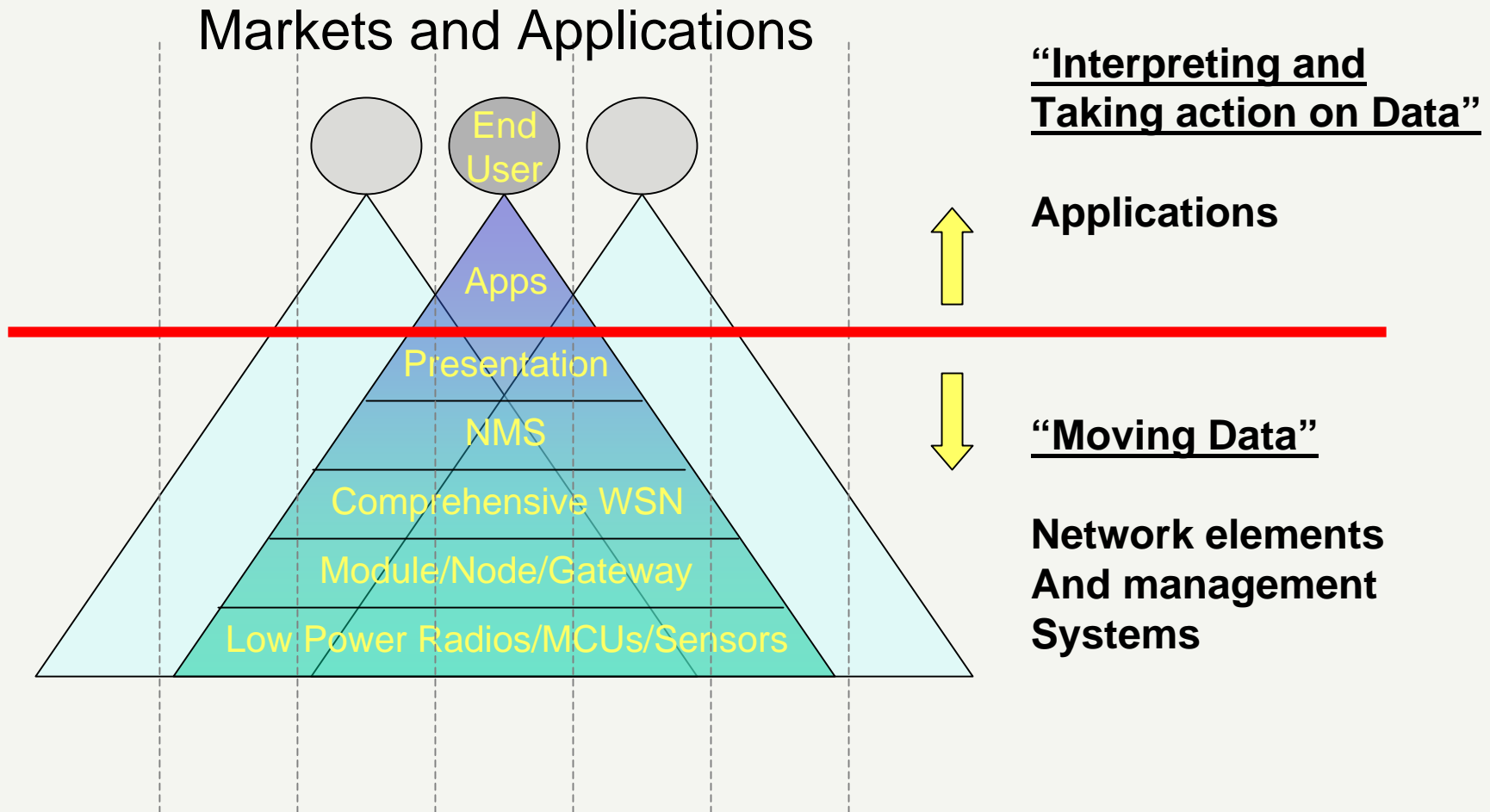
Given the variety and complexity of elements needed to accomplish this, it is essential to begin with a clear understanding of the problem and the customer's priorities to avoid merely delivering technology rather than solving the problem.

What Makes Up An M2M Solution?

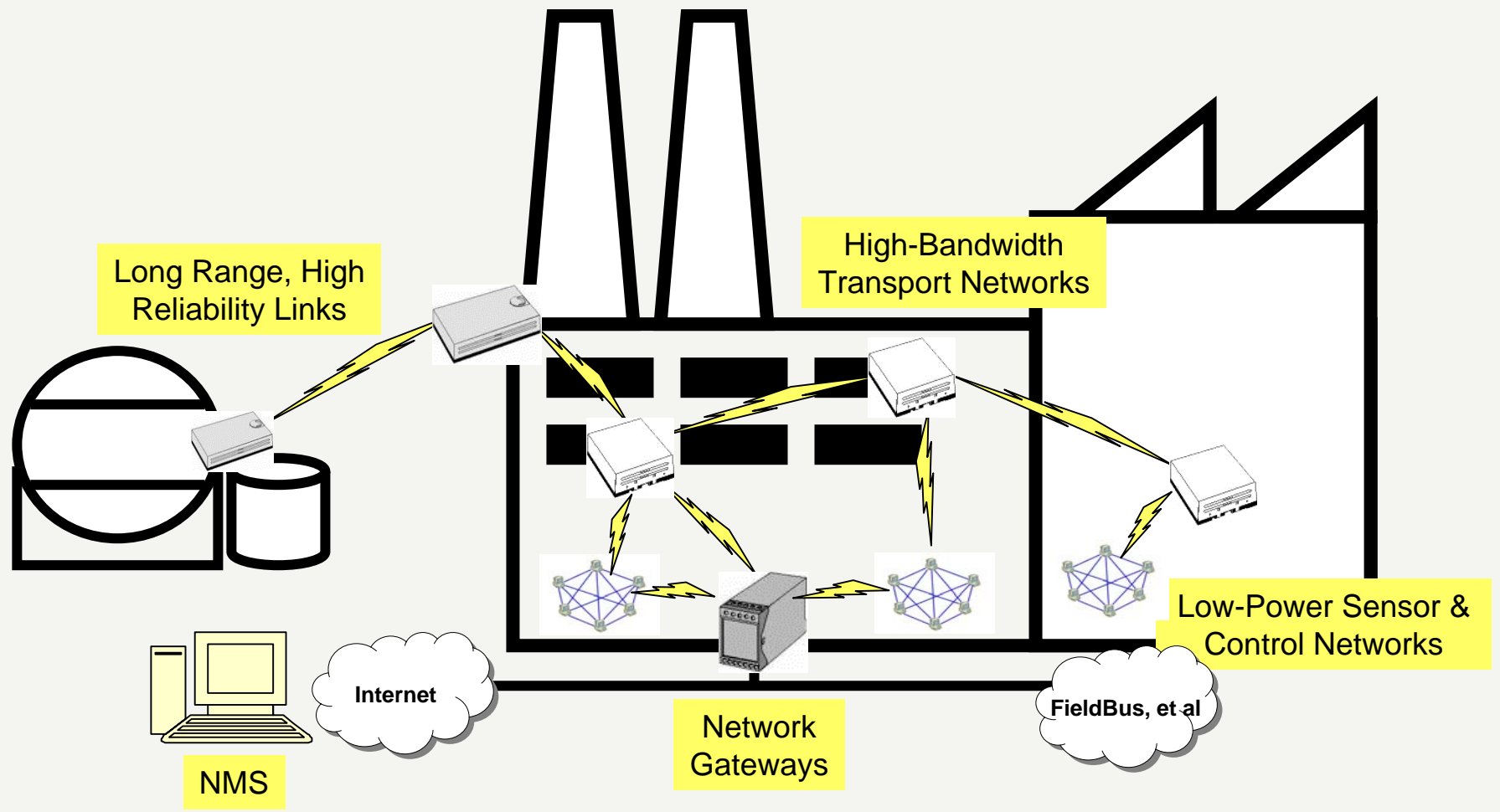
The Solutions-Centric Design Approach

Selecting Your M2M Solutions Vendor(s)

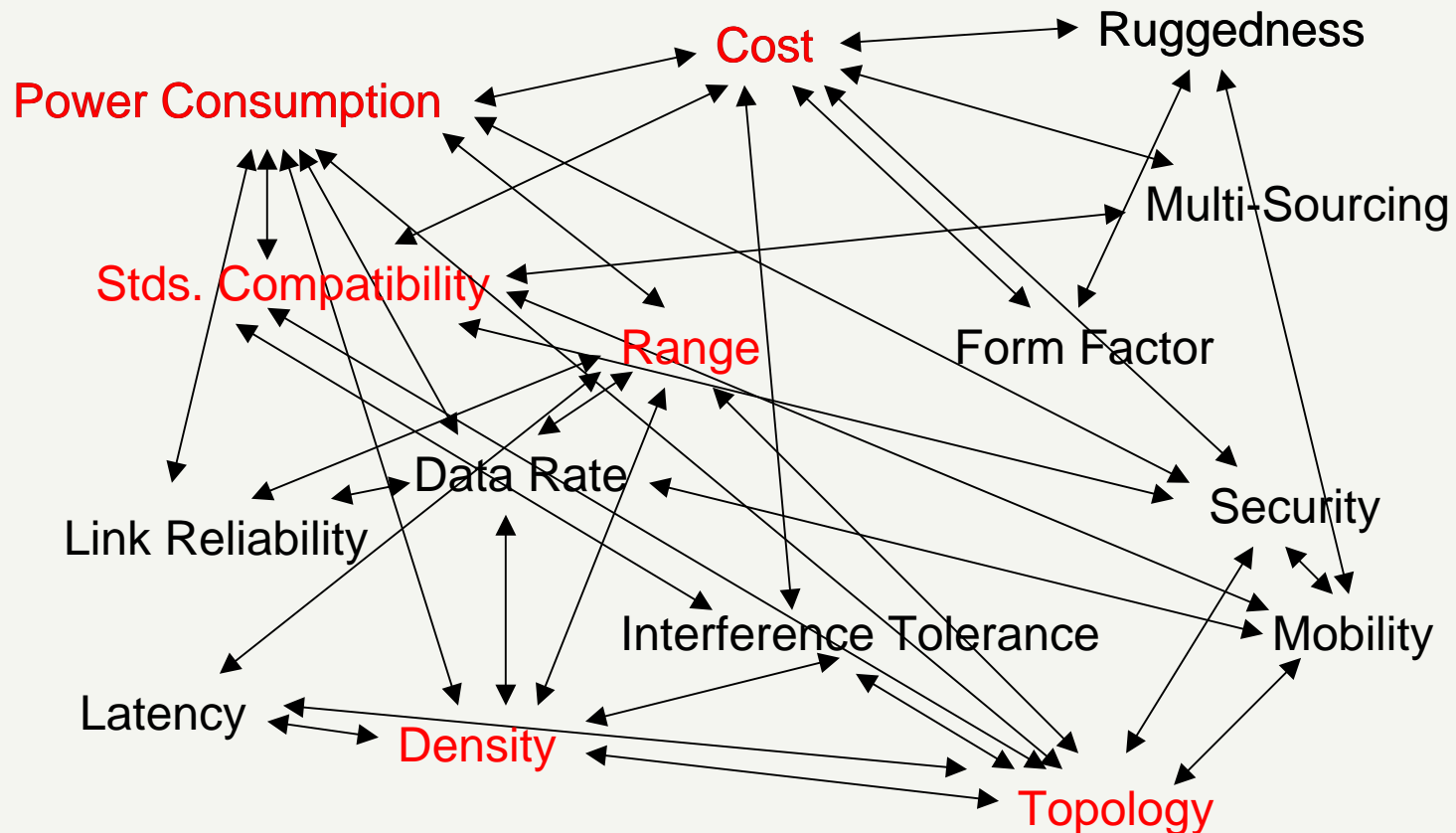
Typical M2M Solution Elements



Wireless Sensors Networks



Wireless Sensor Network Design Trade Offs



Solution-Centric Development

Starts with an understanding of the problem

- *Understand customer's success metric*
- *Prioritize trade-offs*
- *Be sensitive to "human" issues*

Accounts for interactions within the M2M system and the external systems it touches

- *Application and process integration*
- *Network hardware integration*
- *Data, network, and physical security*
- *Network management*
- *System maintenance*

Results in an overall net benefit

- *Solves more problems than it creates*
- *Don't simply measure the direct effects. Account for the indirect impacts as well*

Selecting M2M Solutions Vendors

They should have a clear understanding of the systems nature of an complete M2M solutions

•At least one vendor or you must be prepared to take responsibility for the overall system

They have a clearly defined role and are comfortable and qualified filling it

Their business model can support yours

They have the right technology and/or products

Content-Centric Security (CCS): *Disruptive Authentication for M2M Networks*

Presented by:

David M. Shaw

dshaw@ndsecurity.net

(214)-718-0325

The Nature of the Problem

- *“These tapes were not lost they were stolen,... the theft occurred by altering the electronic manifest in transit ... delivered to the thieves.”* - Stephen Spoonamore, CEO, Cybrinth
- *“No matter how hard you make the initial authentication for the end-user or hacker, the malware can just wait until the authentication is done and then manipulate the transaction.”* – Bruce Schneier, CTO, Counterpane Internet Security
- *“Because the stealing and spoofing is started after the authentication is completed, no amount of fancy log-on authentication would prevent the heist.”* – Roger A. Grimes, Infoworld

M-2-M Issues

➤ Authenticate

- Device
- Application
- User

➤ Boarder Directories

➤ User Directories

➤ Communications

- Secure Session
- Secure setup & breakdown
- Protocol Translations

➤ Architecture

- P-2-P
- Client Server
- Node-2-Node

M-2-M Paradigm Shift

- **Application setup is in the communication protocol**
- **User and machine authentication are setup in the initiating communication session**
- **Predictive link algorithms control subsequent session identifiers**

How the M-2-M paradigm shift is made

- **Initiation machine uses “content-centric” security in its protocol that presents the machine’s identifier, user, application, session key, and session link structure to the receiving machine**
- **Receiving machine’s access control port is to accept a session header which identifies the session and unlocks the secure content within the protocol for deciphering and acceptance**
- **If the session is to be an encrypted/deciphered session, then the key (a component key) is recovered from the secure content header and used to calculate the session key**

How the M-2-M paradigm shift is made

- **The initiation of a session may use any data elements of an existing protocol**
 - **Links from that data to dynamic content-centric security filter**
 - **The content-centric security filter may be placed in any digital carrier medium in a session (requires buffering before processing)**
 - **Works with:**
 - **Wireless**
 - **Landline**
 - **LANs**

- **Initiation session may use distributed component object modules (DCOM)**

Questions?

Presented by:

David M. Shaw

dshaw@ndsecurity.net

(214)-718-0325

“The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects.” - The President's Information Technology Advisory Committee