Perceived Barriers to Industry 4.0 and How to Overcome Them

Tom Craven

VP of Product Strategy

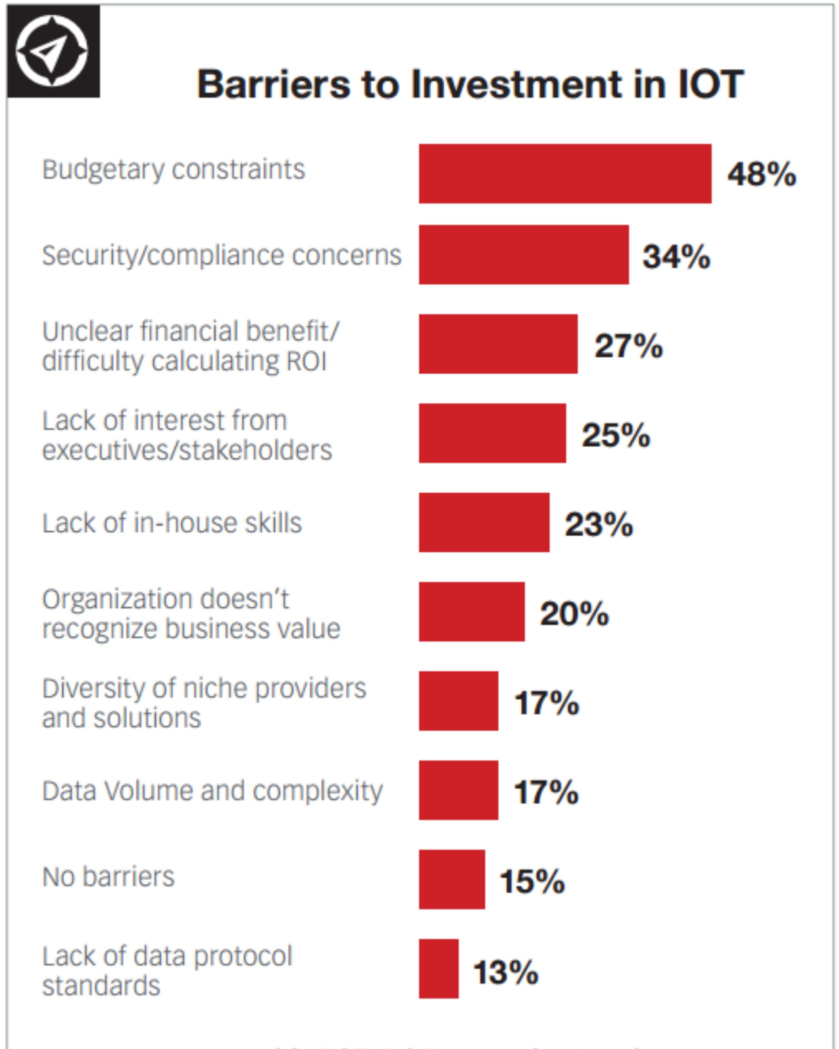
RRAMAC Connected Systems

Overcoming IIoT Barriers

Dell Whitepaper

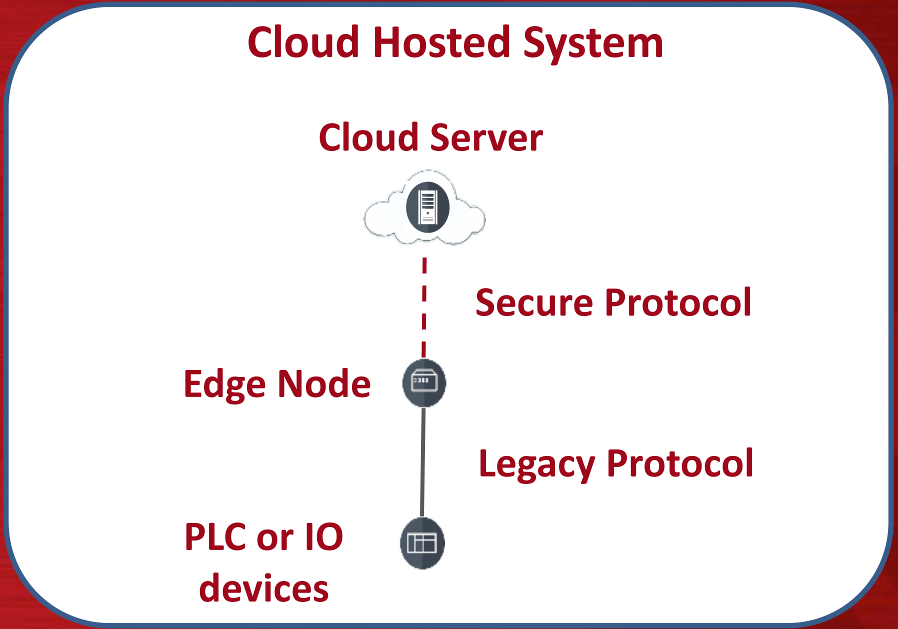
Internet of Things: A Data-Driven Future for Manufacturing

Based on a recent IDG Research survey of 100 IT executives in the manufacturing industry



Lack of Industry 4.0 Standards
A Barrier or Just a Hurdle?

- EdgeNode Functions
  - PLC communication (native protocol)
  - Data buffering and aggregation
  - Secure Connection to Cloud server
  - Controlled access to PLCs



Security matters
Access to existing equipment matters
Specific protocols matter less

Technical Expertise for Industry 4.0

Industry 4.0 should require less expertise, not more. All of these online services are popular because they are easy to use.

- Online Banking
- Online Shopping
- Office 365
- Uber

Industry 4.0 only requires more expertise if you plan to do it alone.

Technical Expertise for Industry 4.0

“Do It Yourself” is often tempting, but is generally not an efficient or cost effective way to implement IIoT

- Advantages of a Cloud based system include:
  - Projects up and running in weeks rather than months or years
  - Leverage existing infrastructure at a fraction of the cost
  - Tier Level 3 Data Center
    - Backup power, redundancy, data backups, controlled access
  - Maintenance and support of servers, database, and connectivity are included

Budget and Timing

- Budgeting
  - Cloud Hosted solutions are a fraction of the DIY costs
  - Operating Expense vs Capital Expenditure
- Timing
  - Very little impact on internal engineering or IT resources
  - Identifiable and measureable ROI
  - No reason to wait until next year

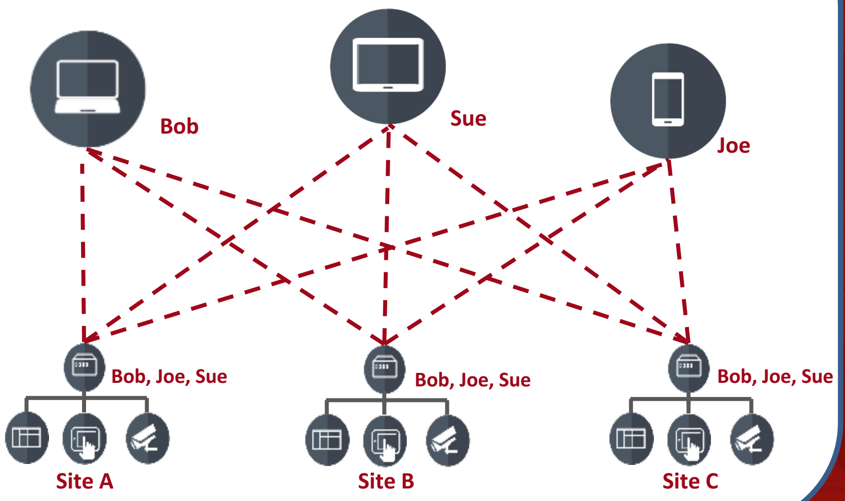
Understanding Security Concerns

- Can anyone on the internet access my equipment?
  - Never use public IP addresses to access equipment
  - Usernames and passwords are not adequate safeguards
- Examples of commonly used internet applications with security:
  - Online Banking and Credit Card Purchases
  - SAP
  - Salesforce.com
  - Office 365
- “Trust No One” may not be the answer
  - TNO can result in unsafe workarounds
  - Proactively manage security

Why VPN is Not the Answer

- VPNs connect a user to a network
- Firewalls need to limit access
- Incoming firewall security hole
- IP Address conflicts between sites
- No Central User Management
- Users must be configured at every site
- Users connect to one site at a time

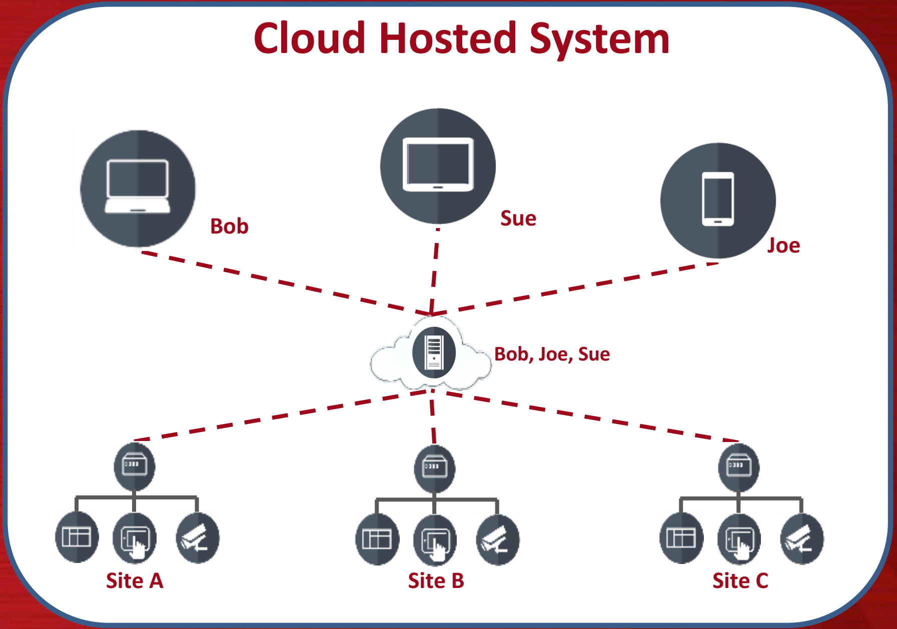
Typical VPN Architecture



A Cloud Hosted Architecture

Centralized User Management

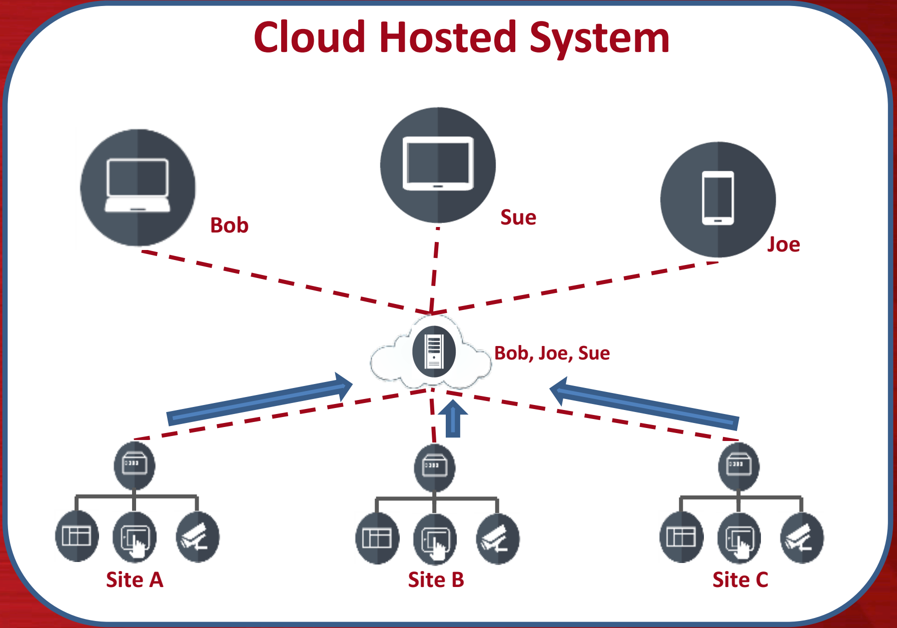
- Unique User Login for every user
- Single login for authorized sites
- Users privileges can vary
- Password rules enforced
- Access is easily revoked
- Temporary access can be granted to subject matter experts



A Cloud Hosted Architecture

Connect Out, Not In

- Connect via open port or proxy server
- SSL/TLS Security Certificates
- AES Encryption
- No incoming VPN access
- Little or no IT configuration changes
- No network browsing by remote users



Defining ROI

- Use a phased approach
- Define measurable revenue and/or cost savings
- Allow for future enhancements
  - Additional data points and/or devices
  - Advanced analytics
  - Easy connectivity to ERP, MMS, etc.
- Limit scope to deliver specific Phase One ROI
- Get bids

Selecting an Industry 4.0 Partner

- Turnkey solutions, not Do-It-Yourself toolkits
- Information at your fingertips, don’t settle for simple data displays
- Connectivity to your controllers as well as ERP, MMS, MES software
- Customized to your application and company
- Experienced provider with expertise and commitment
- Data availability with redundant servers, backup power, offsite backups
- Data security with security certificates, encryption, and user audit trails

Questions?

Tom Craven
VP of Product Strategy
RRAMAC Connected Systems
www.rramac.com
(844) 477-2622