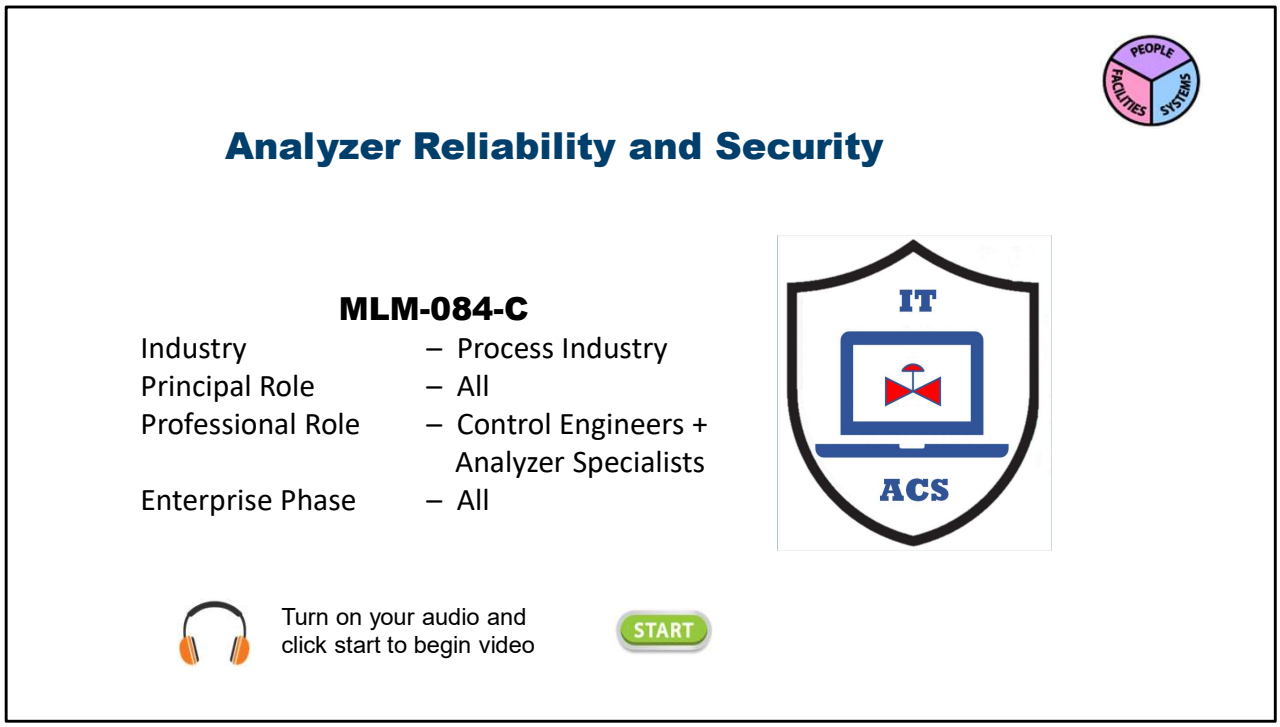
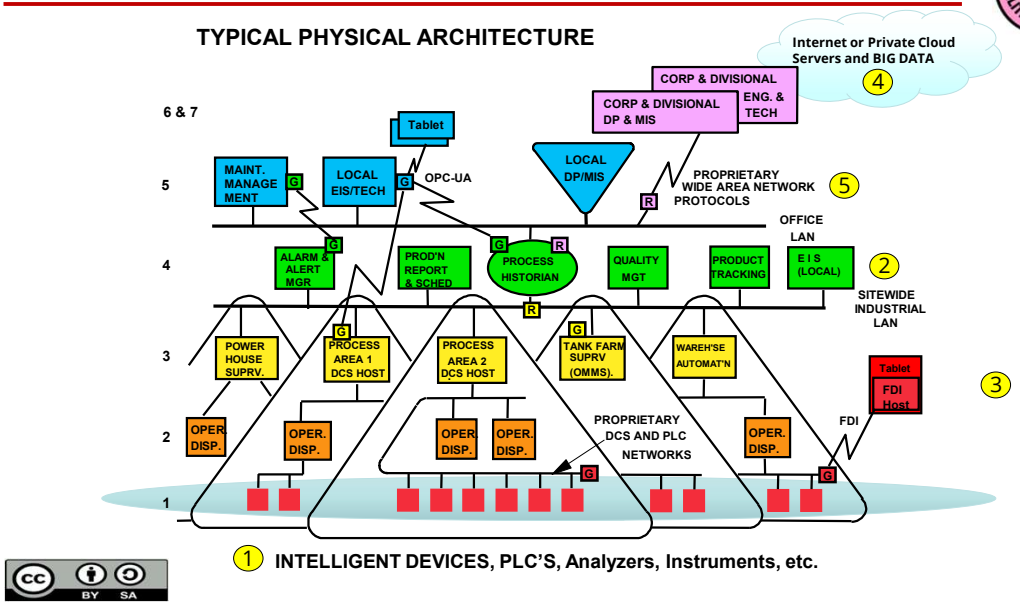


This MLM discusses reliability and cybersecurity measures for analyzers in process Industry plants. It is intended for engineers and analyzer specialists who support these systems.

Click the NEXT button when you are ready to advance to the next slide.

Where do Analyzers Fit in Plant Networks



2

1) Analyzers may be connected to proprietary industrial networks along with PLCs, DCS, SCADA, and local HMIs

2) Manage Engineering and Smart device configuration on an Engineering Information System and use it to detect unauthorized changes

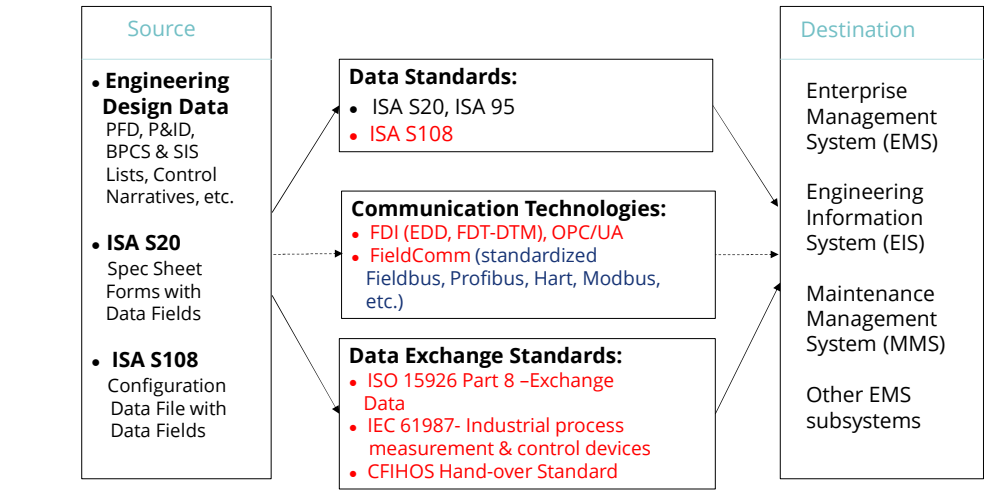
3) Industrial network protocols like FDI will require configuration management software on Engineering Workstations or local tablets

4) Analyzers may need remote support (from vendor or OEM). May even need access from "cloud service" process optimization (like UOP).

5) If so, will need STRONG cyber security to separate remote link from plant control networks.

Communication Protocols & Industrial Standards

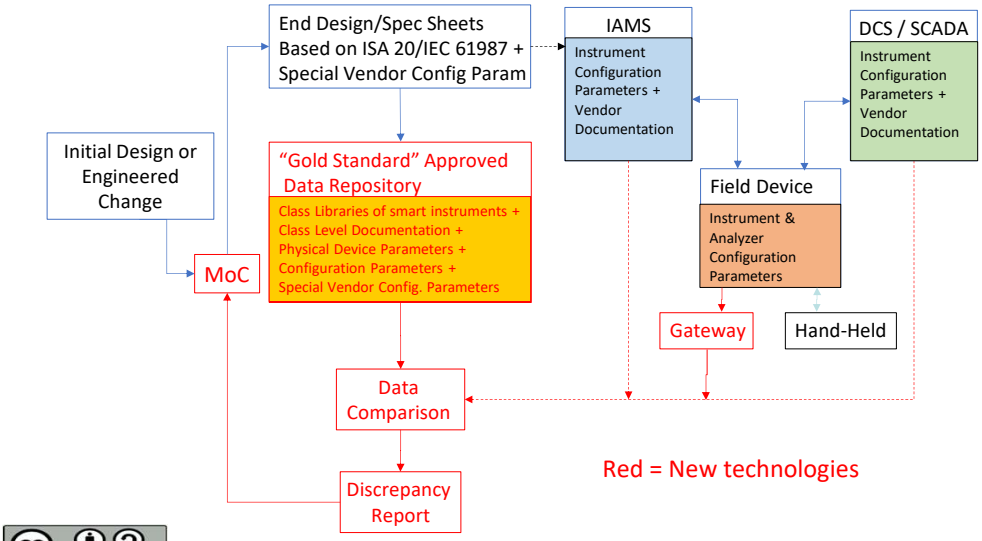
(new Standards in Red)



3

New Data Formats, Communications Technologies, and Data Exchange standards are evolving to move data from design databases to plant operations including EMS, EIS and MMS.

Configuration Management will be Needed



4

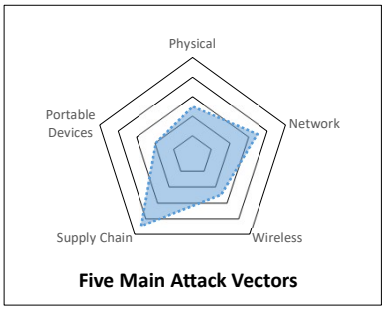
Secure Configurations Management systems are becoming essential to reliable and secure plant operations.

These typically hold design parameters, and accomplish programming and download of changes. They also provide "Management of Change" functions and maintain a "golden copy" of the approved configuration and/or programs contained in field devices including instrumentation, analyzers, PLCs and industrial networks.

They also compare programs installed with the Golden Copy and may manage part numbers and software versions including comparison with bulletins about known bugs and cyber vulnerabilities.

Cyber Security is Essential

- Cyber Security will be a major factor in the rate of adoption of Online Analyzers
- Smart instruments are cheap and powerful, but vulnerable.
- Remote access and “fleet support” is inevitable but dangerous.



Five Main Attack Vectors

Protect Smart Analyzers from the 5 Attack Vectors

- **Physical access** may allow compromise of any software.
- Co-manage **Network** and **Wireless** threats with Plant IT and Instrument Engineers
- Manage **Supply Chain** (Specification and Configuration) with the Instrument/Analyzer Engineer. 30 Mb per device ! Checksums.
- Control access by **portable devices** with Instrument Maintenance and IT.

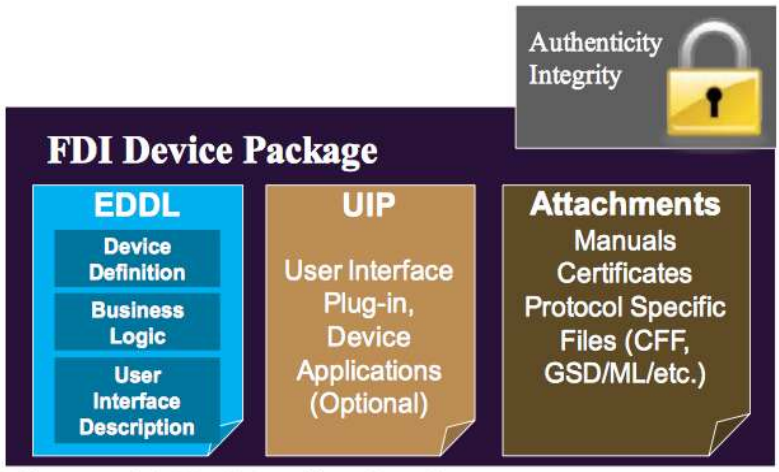
5

5

As examples of these attack vendors, cyber criminals could:

- Steal money by adjusting flow meter and/or quality parameters during a transfer.
- Influence the stock price of a competitor by causing a major environmental release (perhaps at a critical time)
- Hold required quality data hostage (e.g. by encrypting data)

Each IID will Require an FDI Package



A key aspect of Industry 4.0 optimization is direct communication between Intelligent Industrial Devices (IIDs).

As a result, standards developed by Fieldcomm Group, that are designed to promote this communication, will be increasingly important. FieldComm Group are a non-profit organization set up by major control and instrumentation suppliers.

FDI is an Important standard managed by Fieldcomm.

Each FDI Device Package contains 4 sections that define how it communicate with other IIoT devices:

1. Authentication Integrity (insures, like a “veri-signed device driver”, that the source is trusted, and the package is unchanged since it was sent)
2. EDDL – Standard defines device communication protocols
3. UIP – Optional Applications interface for device.
4. Attachments (Manuals, Certificates, etc., in a Authenticated and locked file.

Together, these Packages provide tens of megabytes of information on each IID

Key “Take-away” Messages

- Analyzers must fit within existing plant Control and Information Architectures, and Engineering & Maintenance practices
- The selection of new Intelligent Device communication standards will be critical, particularly around communications.
- Cyber Security will be a “gating item” controlling the rate of adoption.
- Distribution of Industrial Intelligent Device information will be electronic, standardized, and massive.

Please click here to provide feedback on this MLM.

7

The following are Key Messages to “take away”

- Analyzers must fit within existing plant Control and Information Architectures, and Engineering & Maintenance practices
- The selection of new Intelligent Device communication standards will be critical, particularly around communications.
- Cyber Security will be a “gating item” controlling the rate of adoption.
- Distribution of Industrial Intelligent Device information will be electronic, standardized, and massive.

Author

Gary is president of Enterprise Consultants International (ECI) since 2000, offering master planning, project management and metrology services to industrial clients.

He is also active in promoting PERA enterprise management concepts, and is working with international standards bodies to develop industrial enterprise information and control standards.

Gary has over forty years experience in the automation and operation of process manufacturing facilities. He is experienced in the application of control and information systems including; Site-Wide Process Optimization, Complex Batch Operations and many process analyzer systems including a custody transfer analyzers and approximately 100 Power Plant Continuous Emissions Stack Monitoring Systems (CEMS).

He has also been responsible for design and implementation of 25 technical computing systems including Engineering Information Systems (EIS), and Engineering Automation Systems (EAS) ranging from the second engineering CAD system in Canada, to the latest EIS and EAS systems implemented in world-scale projects with thousands of users.