ISA100 WCI Webinar

Webinar date: 04. October 2023

Cyber secure and SIL2 capable wireless safety

Presenter:

Ådne Baer-Olsen
Adne.Olsen@draeger.com

About the Speaker

Ådne Baer-Olsen

Global BDM Lead Wireless safety

Draeger AG

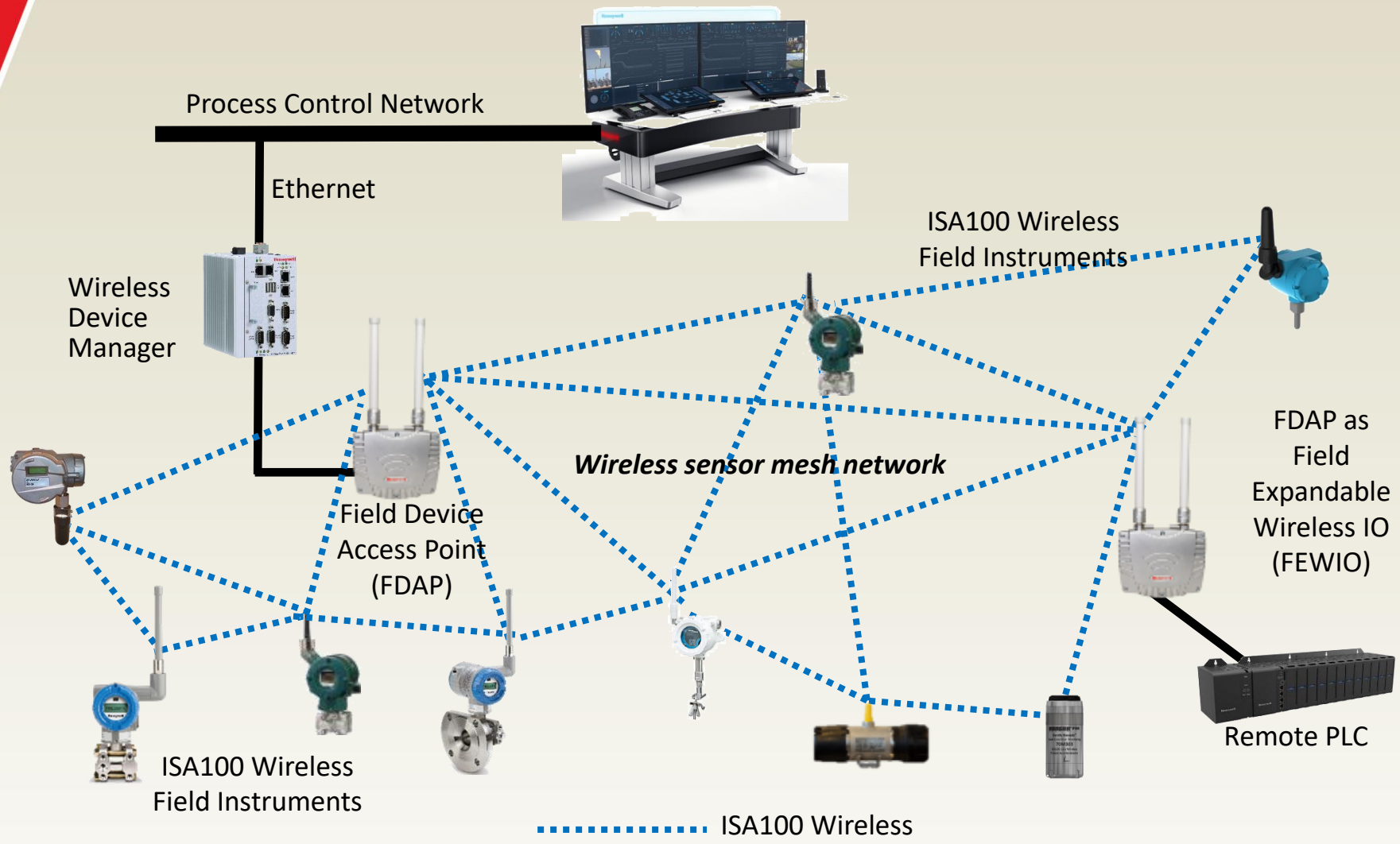
Ådne has almost 20 years' in the Detection and automation industry and is regarded as a specialist in his field. He has been instrumental to the rise of wireless gas detection systems. His team designed and delivering the first Wireless SIL2 gas detection system in the world offshore Norway. Also as part of Drager suppling the first wireless systems to the Middle East and Africa. Currently he is globally responsible for all wireless safety systems within Dräger.

Among his significant positions, Ådne has is the Leader of WCI in Europe and Middle East promoting ISA100. Providing invaluable support, training, and expertise to major oil and gas operators

Agenda

1. Introduction Industrial Wireless
2. ISA100 Wireless Industry Standard
3. Cyber security
4. Safety/ control application
5. Case Study
6. Summary

Introduction to Industrial Wireless



Applications examples

- Machine health monitoring
- Basic process control
- Monitoring of well heads
- Remote process monitoring
- Leak detection monitoring
- Diagnosis of field devices
- Condition monitoring of equipment
- Environmental monitoring
- Tank level monitoring
- Gas detection
- Fuel tank gauging
- Steam trap monitoring
- Open loop control
- Stranded data capture
- And more

ISA100 Wireless Fast Facts

- International standard IEC 62734 since 2014
- Complies with ETSI EN 300 320 v1.8.1 (LBT)
- End-User Driven Standard - meeting all current and future industrial needs
- Sensor routing or field routers for best performance – Freedom of choice
- Broad Multi-Vendor Portfolio of ISA100 Wireless Devices
- ISA100 Wireless enables SIL-2 Certification
- Ensured Interoperability - best-in-class solutions from best-in-class suppliers
- Readily available ISA100 Wireless Modules and Stacks
- Enable fast-track development and go to market

Benefits of ISA100 Wireless Instrumentation

Cost Savings	• Up to 90% of installed cos of conventional measurement technology can be for cable conduit and related construction • Typically: 1/2 the costs, 1/5 of the time • New and scaled applications are now economically feasible
Improved Reliability	• Wired sensors may be prone to failure in difficult environment • Wireless can add redundancy to a wired solution
Improved Visibility	• Condition monitoring of secondary and remote equipment • Process monitoring, fast additional data for trouble shooting
Improved Control	• Add wireless to existing processes for more optimal control
Improved Safety	• Safety related alarms - end to end SIL2 certifiable

ISA100 Wireless Product Portfolio

Infrastructure

Independent Gateway
- Honeywell, Yokogawa

Access Point (AP)
- Honeywell, Yokogawa

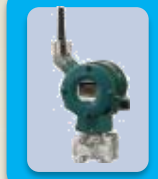
Integrated Gateway/AP
- Honeywell, Yokogawa, CDS, Nexcom

GW/AP + Recorder
- Yokogawa

Adapter (HART, etc.)
- Honeywell, Yokogawa

Measurement & Control

Temperature
- Honeywell, Yokogawa



Pressure / Flow
- Honeywell, Yokogawa

Level
- Honeywell, Yokogawa

DI/DO, AI
- Honeywell, Yokogawa

Valve Position
- Eltav, Flowserve, Honeywell

HSE + Life cycle

Corrosion
- RCS , Honeywell

Steam Trap
Spirax Sarco, TLV, Armstrong, Bitherm

Vibration
- GE's Bently Nevada, Divigraph

Gas
- GasSecure, Scott Safety, New Cosmos, Riken Keiki

pH
- Honeywell, Yokogawa

Agenda

1. Introduction Industrial Wireless
2. ISA100 Wireless Industry Standard
3. Cyber security
4. Safety/ control application
5. Case Study
6. Summary

Cyber Security?

This is generally an high concern for end users

Wireless 802.15 (ISA100)

Threats to security of field wireless systems: Sniffing

Threats to security of field wireless systems: Data Falsification

Threats to security of field wireless systems: Spoofing

Threats to security of field wireless systems: Replay Attacks

Security functions of ISA100

	Wireless Threats			
Wireless Defence	Data Sniffing	Data Delay / Replay	Data Falsification	Data Spoofing
Data Encryption	**Secure**	Not Secure	Not Secure	Not Secure
Device Authentication	**Secure**	Not Secure	**Secure**	**Secure**
Data Authentication	**Secure**	**Secure**	**Secure**	**Secure**
Data Freshness	Not Secure	**Secure**	Not Secure	Not Secure

ISA100 Wireless has 128bit AES encryption

- 64-bit keys have about a million trillion possible keys. Max speed brute attack today would take about a second
- 128-bit keys might seem vulnerable in that respect only being twice the number of 64-bit
- Not so fast. There are around 32 million seconds in a year. 32 million is
  25 doublings.
- So if you can crack a 64-bit key in a second it will take a
  year for an 89-bit key (64 + 25). A million is 20 doublings, so an 109-bit key will take a million years

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Moore’s law

Moore’s law says that computers get twice as fast every 2 years
In cryptography terms that means that advances in computer power will give you one extra bit every two years. That is, if you can crack a 64-bit key in a second this year, you should be able to crack a 65-bit key in a second 2 years later.

On that basis increases in computer power would bring the time to crack a 128-key down to one year 78 years from now and 128 years to bring it down to a second.

Given that our conservative estimates are orders of magnitude better than what can actually be done, we can conclude that 128 bit encryption is absolutely safe for the rest of the century from known technology.

.

Bottom line

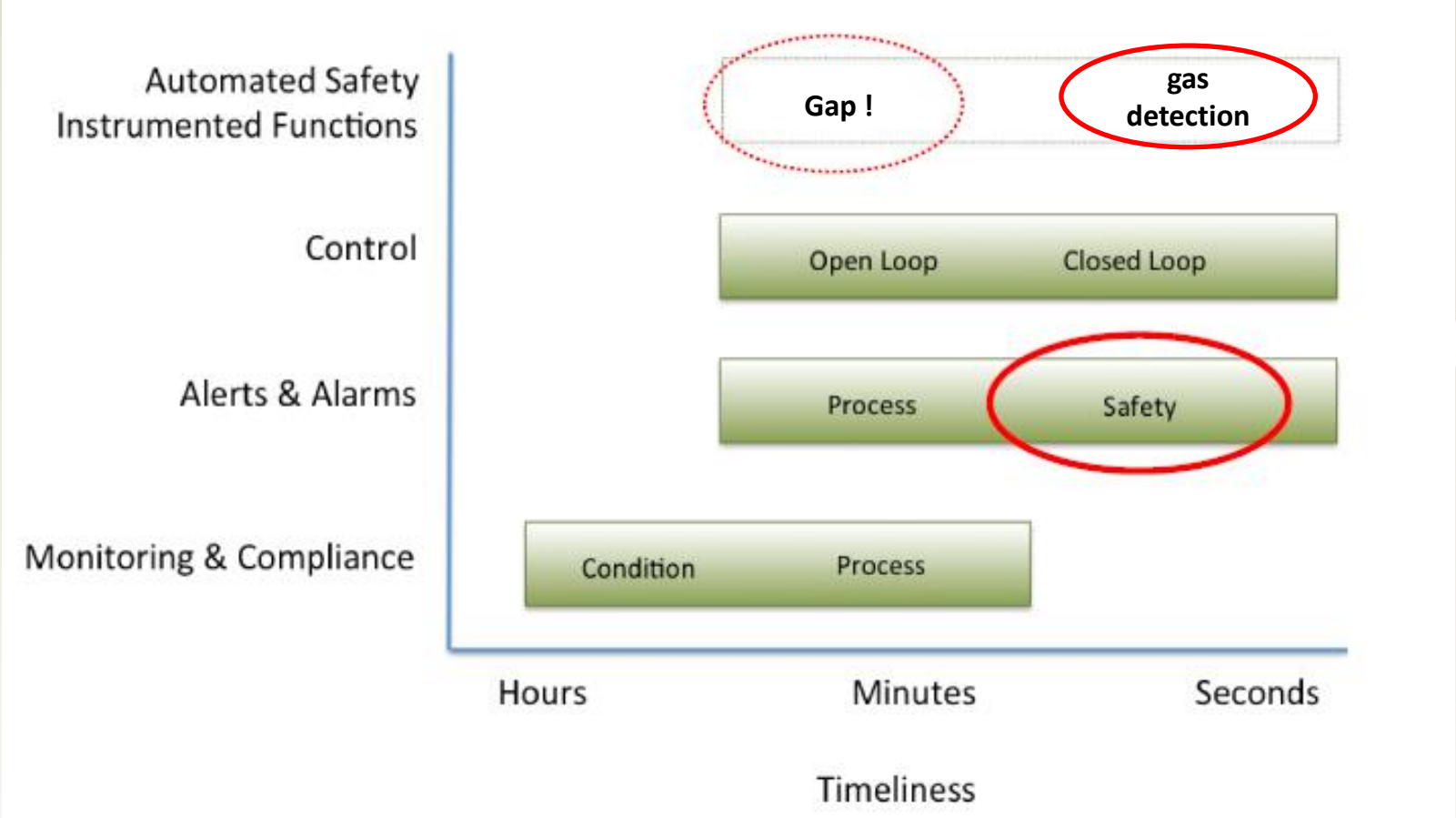
With 128-bit AES encryption you can relax — there are other things much more serious to worry about.

Jamming

Agenda

1. Introduction Industrial Wireless
2. ISA100 Wireless Industry Standard
3. Cyber security
4. Safety/ control application
5. Case Study
6. Summary

Safety/ control application



Multi protocol communication

ISA 100 WIRELESS

OPC UA

PROFIsafe

HART COMMUNICATION PROTOCOL

Modbus

PROFINET®

Wireless in Safety Applications

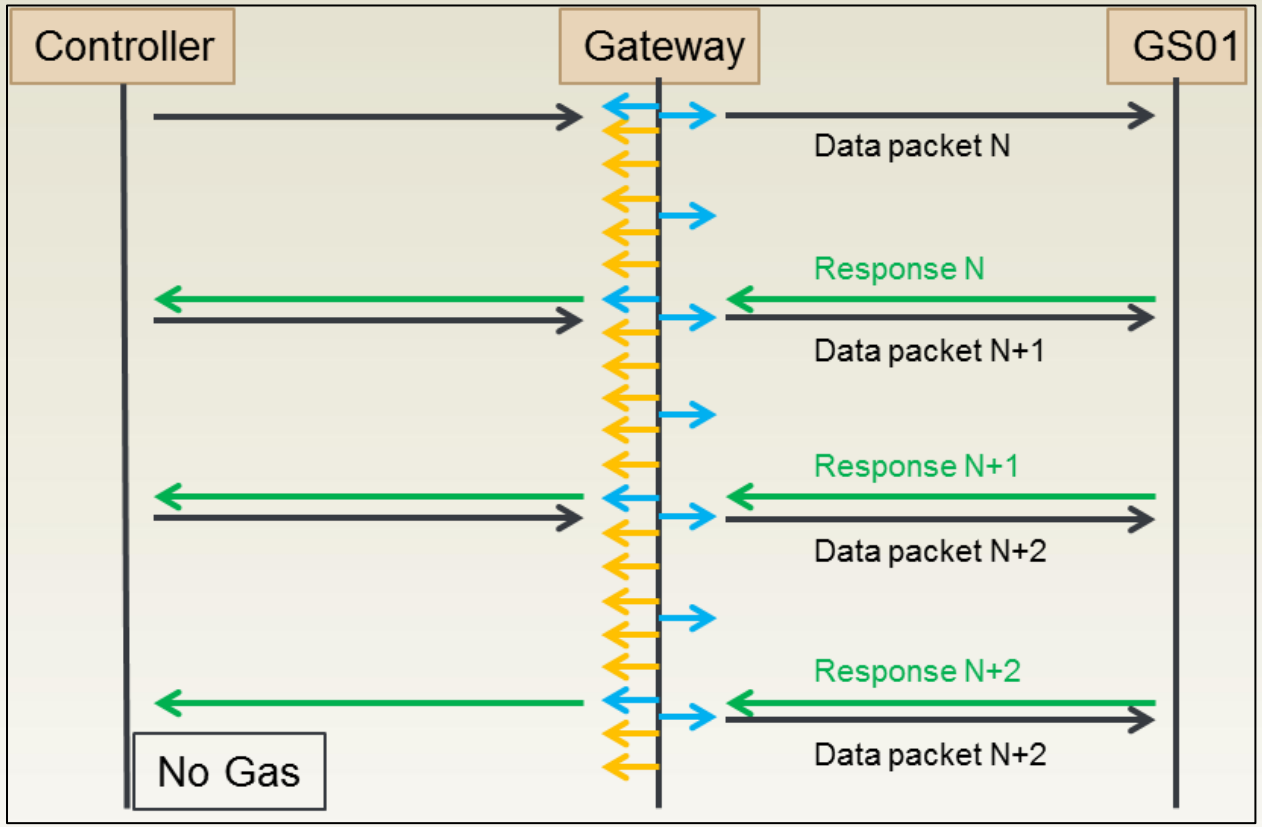
Design & performance criteria

- High availability
  - No lapse in detection coverage due to “blind” times or loss of packages
  - Communication patterns that allow for fast response times – **balanced with battery lifetime** for wireless applications
- High reliability
  - Reliable detection technology with no false alarms
  - Long maintenance intervals, little/no drift in between test intervals
  - Suitable for use in **SIL applications**

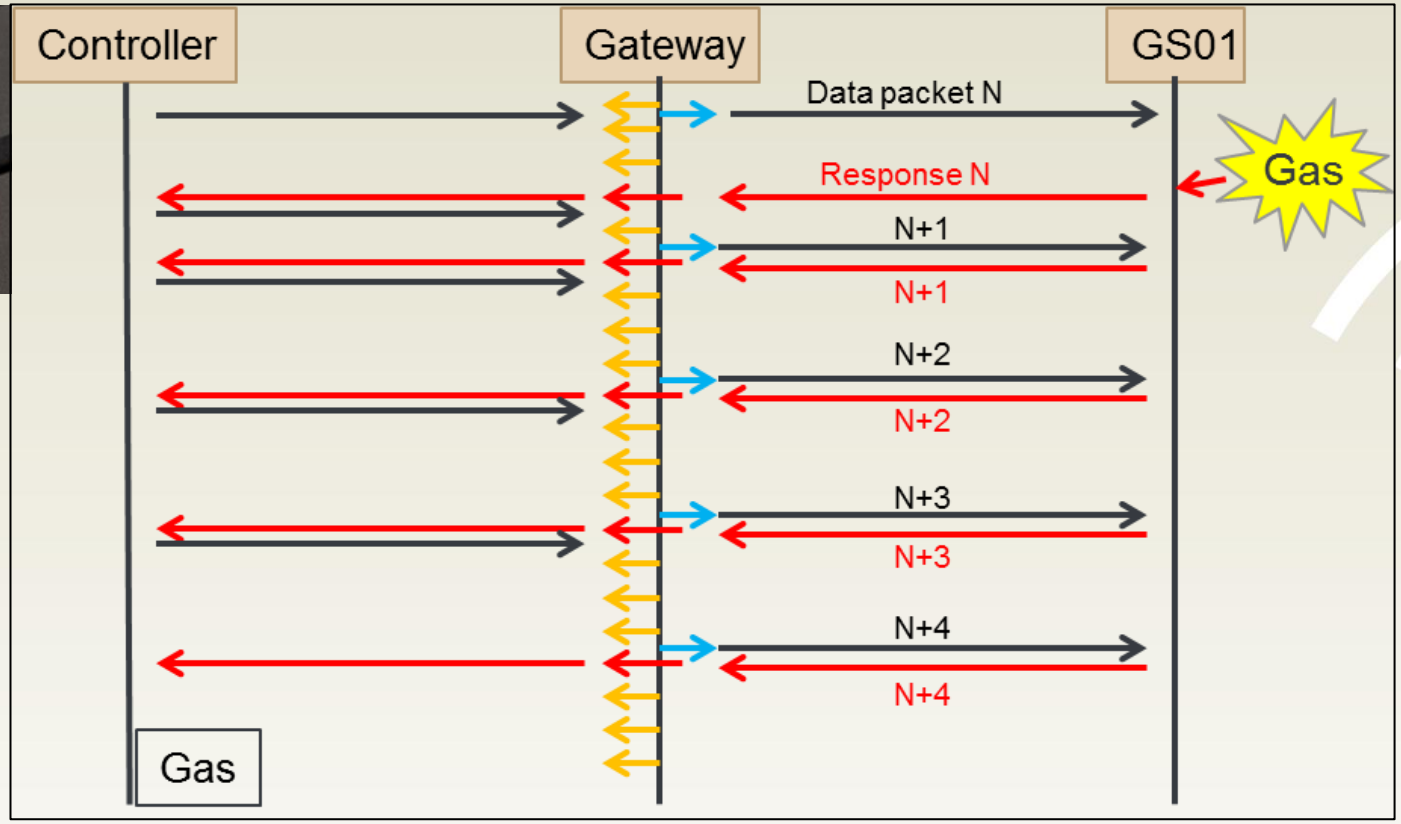
⇒ Safety protocol – deployment environment – configuration

Wireless Networks in Safety Applications

requirements for **long battery life** with **acceptable response time** – a trade-off?



Wireless Networks in Safety Applications



Wireless Networks in Safety Applications
Criteria for network protocols

- End-to-end **safety protocol according to IEC 61784-3** is required in SIL environments, which means that
  - Tunnelling/mapping of foreign safety related protocols such as PROFIsafe through the network is needed

- Quality of Service through limits for bandwidth, latency, and **priority** is ensured
- Integrity/**secure** (encrypted) wireless communication is provided
- Device **interoperability** supports communication of devices from multiple vendors on one network is feasible

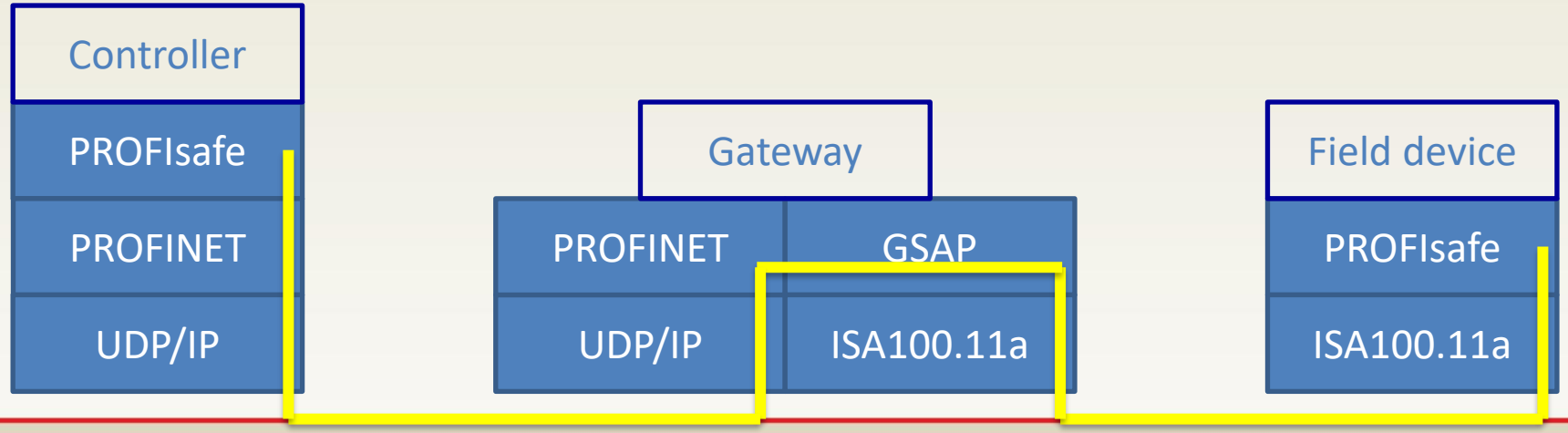
- ISA100.11a provides for all of this!

Wireless Networks in Safety Applications
Criteria for network protocols

PROFIsafe is a safety related profile **defining application specific functionality** on top of PROFINET. PROFIsafe is SIL3 certified!

Black channel principle

- Independent of the communication method
- Covers the entire communication path from the sensor to the controller – the gateway needs to support PROFINET
- Protects for eventual failures in communication wrt to SIL capability



Wireless Networks in Safety Applications

Criteria for network protocols

Error-handling mechanisms addressed by PROFIsafe: Safety-related protocols need to be able to mitigate a range of errors if used in SIL environments:

Failure/Remedy	Sequence Number	Time-out with Receipt	Codename for Sender and Receiver	Data Consistency Check
Repetition	X			
Deletion	X	X		
Insertion	X	X	X	
Resequencing	X			
Data Corruption				X
Delay		X		
Masquerade		X	X	X
FIFO failure		X		

Only the combination of **ISA100.11a and PROFIsafe** currently allows us to implement all 4 mechanisms!

Bottom line:

exida

The manufacturer may use the mark:

exida CERTIFIED IEC 61508 SIL 2 CAPABLE

Valid until April 30, 2018
Revision 1.0 March 31, 2015

ANSI

ANSI Accredited Program
PRODUCT CERTIFICATION
#5004

Certificate / Certificat
Zertifikat / 合格証

GasSecure 1311056 P0034 C001

exida hereby confirms that the:

GS01 Wireless Gas detector
HW version GS01_A3 and GS01_A7, SW version 3.0.0

GasSecure AS
Oslo, Norway

Has been assessed per the relevant requirements of:

IEC 61508 : 2010* Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 2 (SIL 2 Capable)

Random Capability: Type B Element

SIL 2 @ HFT=0; Route 1_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The GasSecure GS01 Wireless Gas detector will check for the presence of Methane / Propane in normal ambient air and make the measurement result available to a control system.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.
*) See PROFIsafe comment on page 2.

Evaluating Assessors

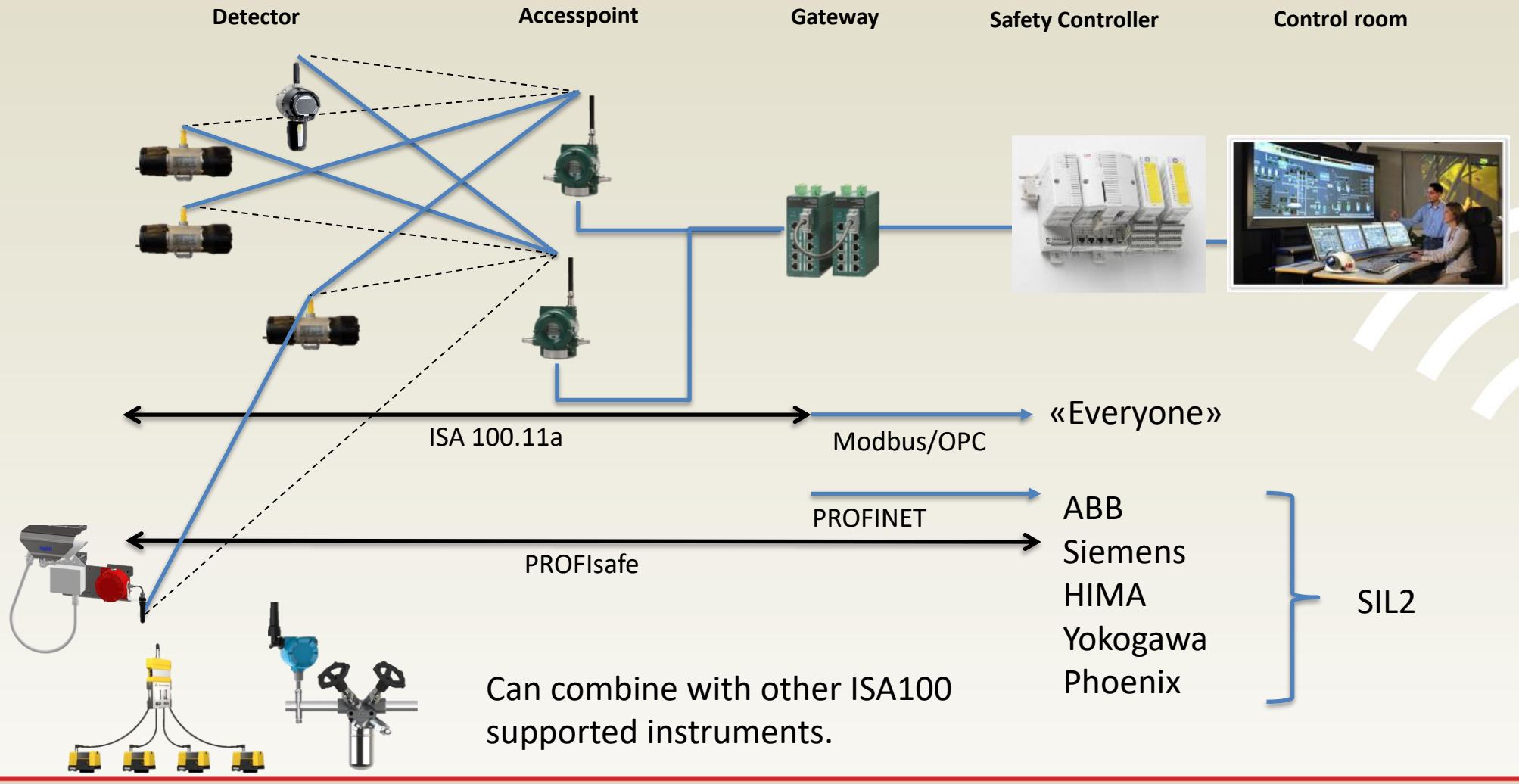
Michael Medoff
Certifying Assessor

Page 1 of 2

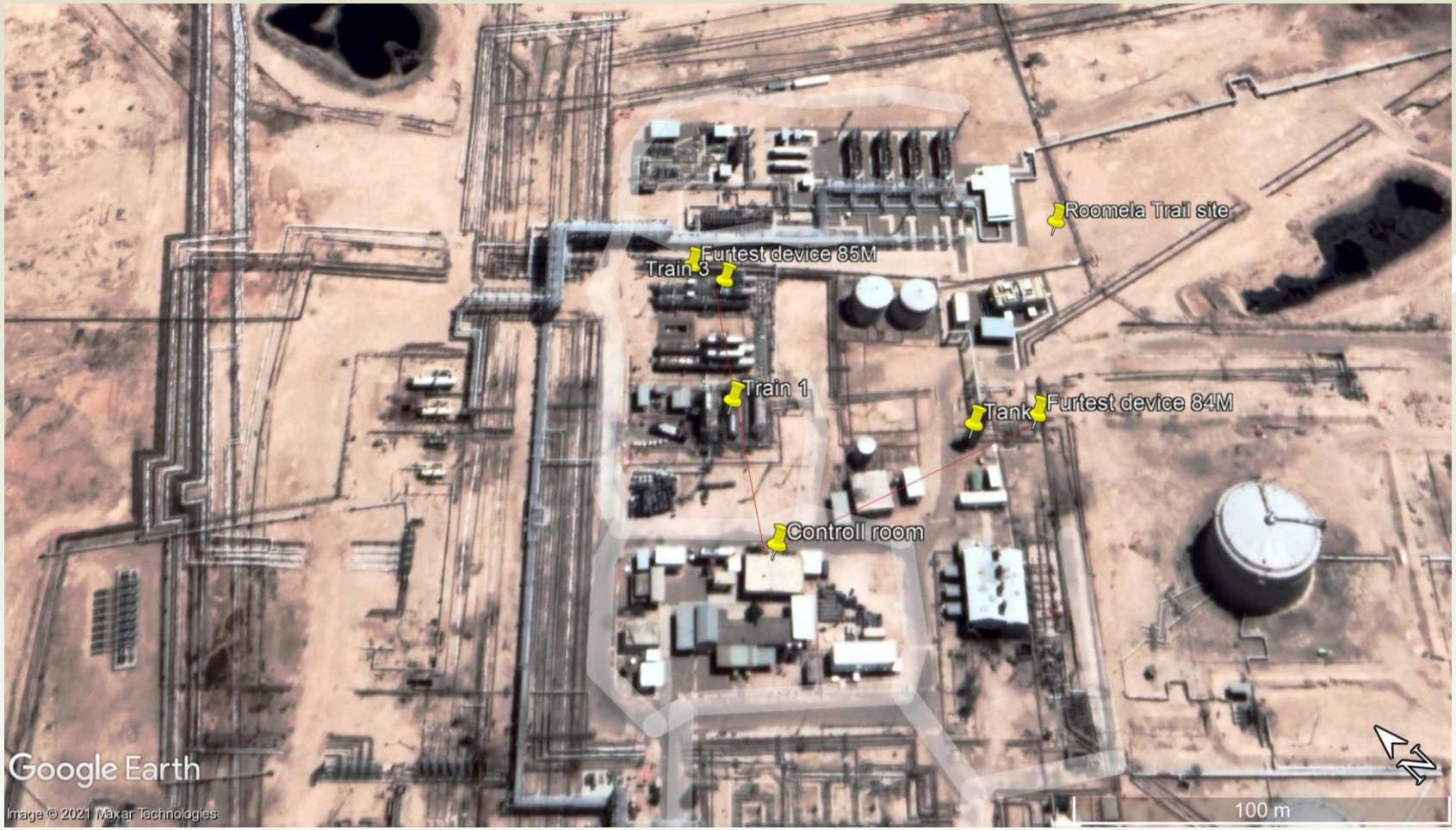
Agenda

1. Introduction Industrial Wireless
2. ISA100 Wireless Industry Standard
3. Cyber security
4. Safety/ control application
5. Case Study
6. Summary

Communication



Case study


Roomela Trail site
Furtest device 85M
Train 3
Train 1
Tank
Furtest device 84M
Controll room
Google Earth
Image © 2021 Maxar Technologies
100 m

Requirement for fast deployment

Wireless Gas Detectors

Access Point

Control System

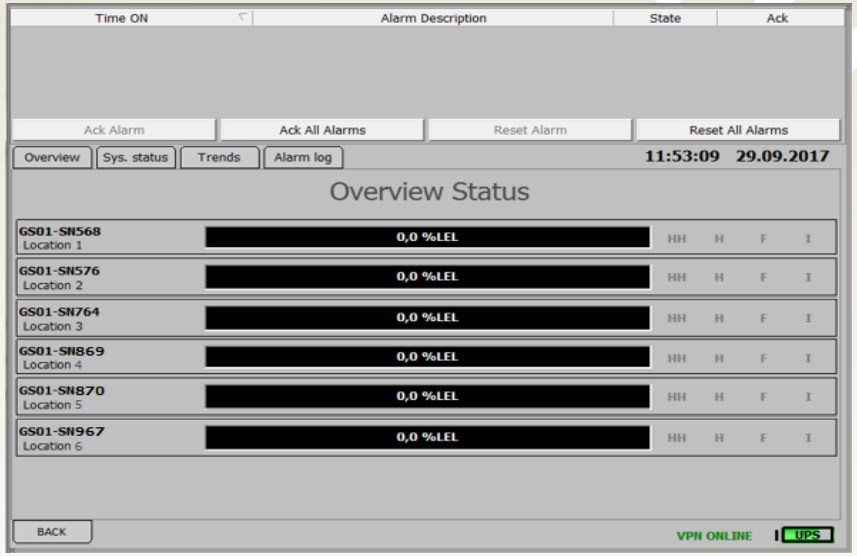
* Optional mobile radio antenna for remote access

System overview

- Standalone solution, requiring only main power supply.
- Accommodates up to 20 GS01 wireless gas detectors
- An HMI provides full overview of alarms, gas measurements, diagnostics data, trends and system status.

- The system is pre-configured to user application and requirements, and assembled and tested prior to delivery. The user only installs the field equipment and connects power to the system.

- **Complete solution** – Includes PLC, HMI, all software and settings preloaded for easy commissioning even in remote locations.
- **Industry-standard interfaces** – Facilitates integration to higher control systems and integration of 3rd party equipment.



After successful Trial

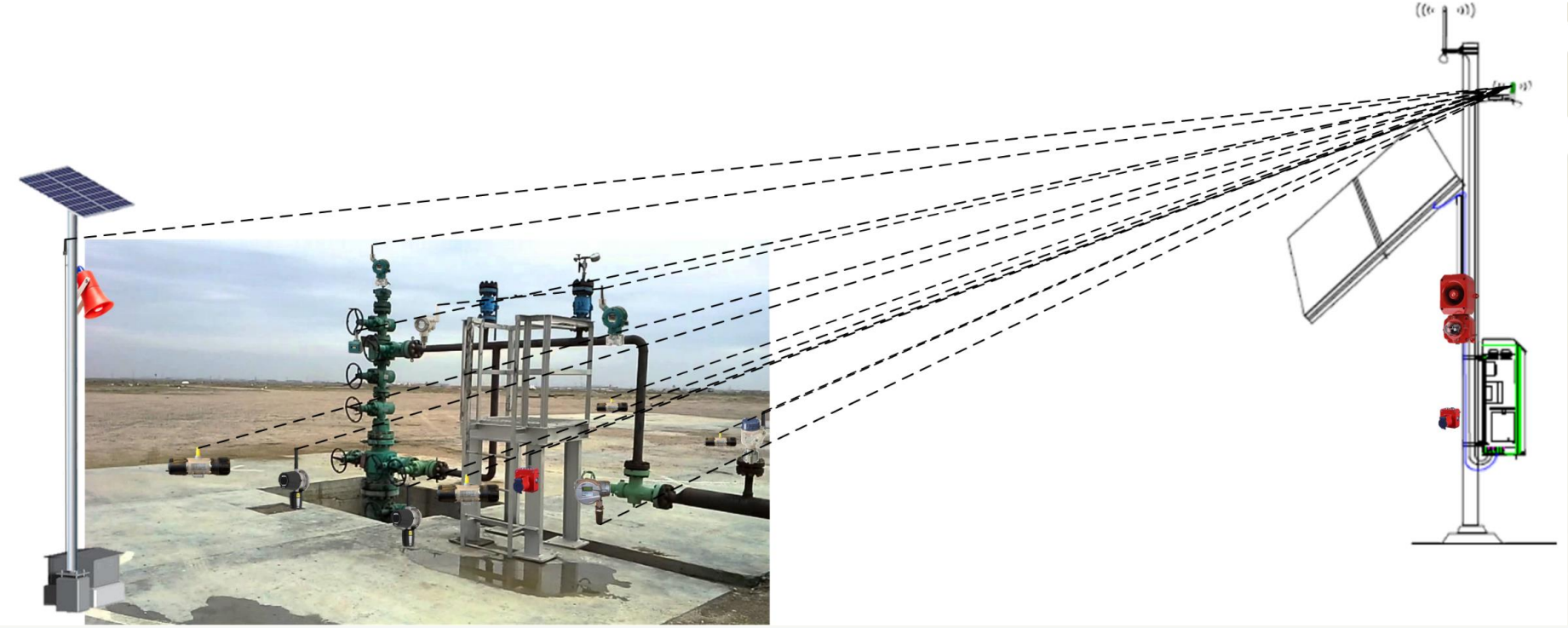
Battery Powered / Wireless Communication

Locally Powered / Wireless Communication

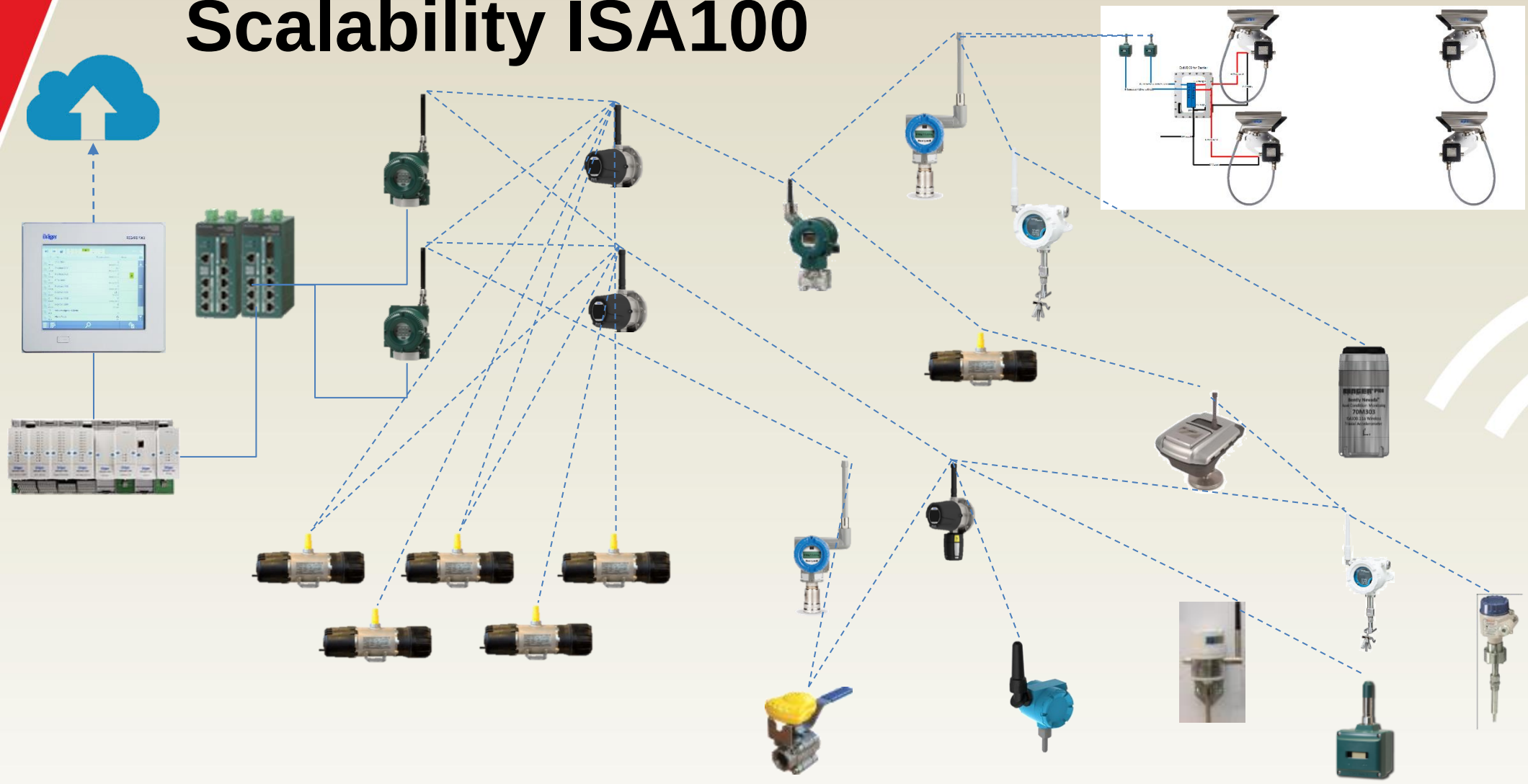
New Products for Wireless Solutions

Field options

Ref#	Technology	Ref#	Technology
1.	Wireless sounder & beacon, solar power: Safety	6.	Wireless MCP for local operator and control room info
2.	Wireless pressure transmitter: Enhanced operation information.	7.	Wireless valve position monitor
3.	Wireless detection. HC and Toxic. Local safety and operational safety.	8.	Wireless flow monitor
4.	Repeater for enhanced coverage	9.	Wireless corrosion monitoring
5.	Wireless temperature for process information	10.	Wireless inductive sensor: Pig arrival or other sensing



Scalability ISA100



ISA100 Wireless Adoption Development Eco-system

WCI ISA100 Wireless Rapid Development Kit

- Everything you need to develop an ISA100 Wireless (IEC 62734) connected field instrument
- Develop ISA100 Wireless (IEC 62734) compliant and certifiable field instruments with minimal effort using application layer code provided
- Includes reference hardware design for ISA100 Wireless (IEC 62734) field instrument implementation
- Certified WISA modules run ISA100 Wireless communication stack
- User friendly SPiN development board includes OLED display and a large variety of sensors

https://centerotech.com/product/wci-isa100-rapid-development-kit/

Online Resources

www.isa100wci.org

- Learning Center with White Papers
- Articles, End-user stories, Forum
- Receiving over 20,000 web views per month
- Full list of certified/registered ISA100 Wireless devices
- And more useful content for you and your business

ISA100 Wireless Interest Group

- Latest news, end-user and expert discussions, insights
- 1100 members and growing; please join and invite your peers to join as well !
- Receiving over 5,000 web views per month
- Limited Time Offer: Join the group and you will be entered in a prize draw to win a new iPad

ISA100 Wireless

For Your Attention!

Questions?

Ådne Baer-Olsen
Adne.Olsen@draeger.com