Lessons Learnt developing Industry 4.0 solutions

Down load a copy at www.northerncrucible.co.uk

NORTHERN CRUCIBLE
A MELTING POT OF IDEAS FOR MANUFACTURERS

Lessons Learnt developing Industry 4.0 solutions

Mike Brrows

Senior Advisor Industry 4.0

Contents

01 Who am I?

02 Back ground

03 Market

04 Lessons Learnt RS IIoT Journey

05 Don’t Forget

01 Who am I?

British COAL

MONITION LTD
The advantage of knowledge

EMERSON
Process Management

MONITION
Reliability and Condition Monitoring Services

RS Monition
Asset Reliability and Condition Monitoring

EUROPEAN COMMISSION

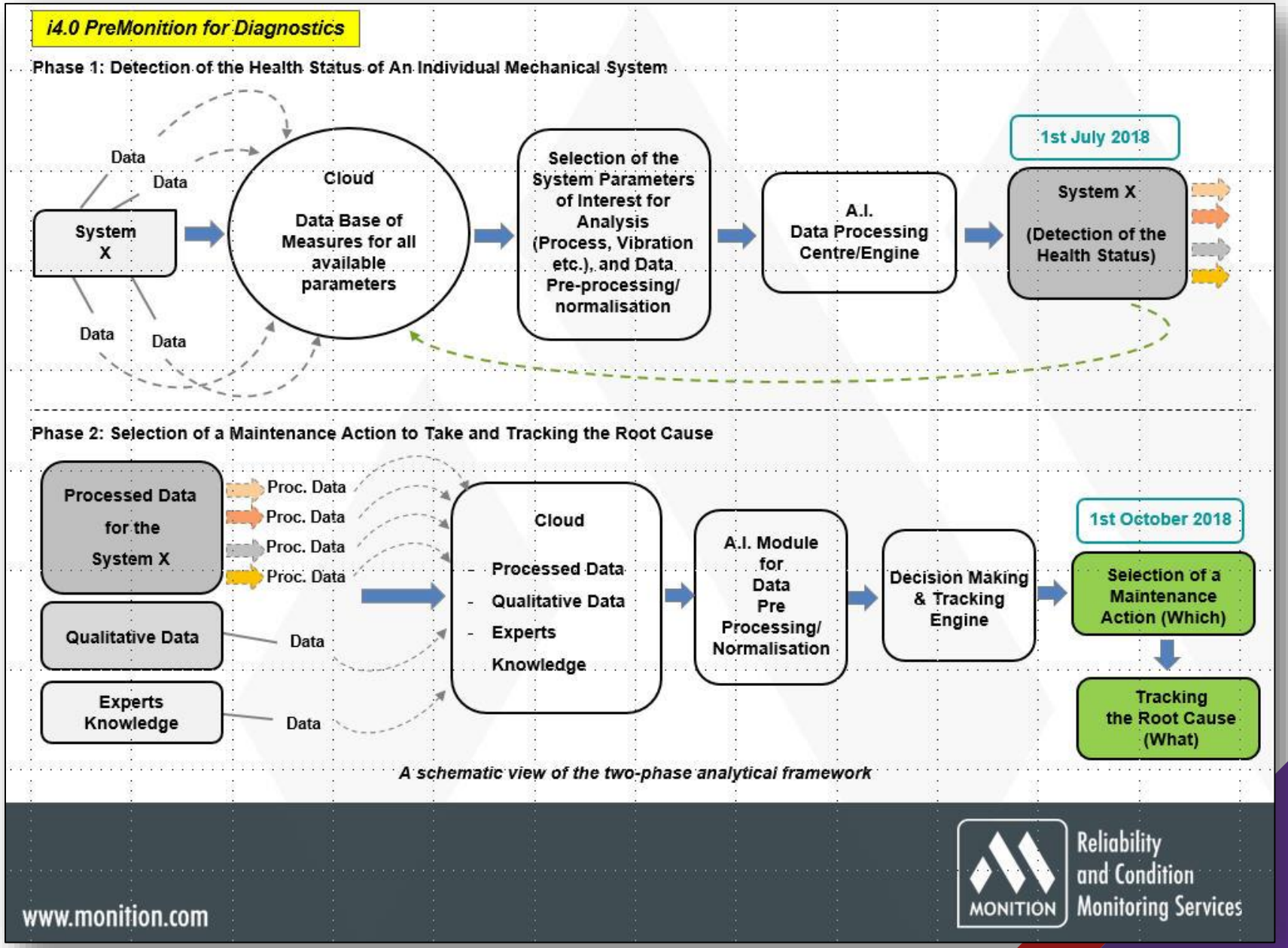
Innovate UK

INDUSTRIAL STRATEGY

Monition i4.0 Intelligent Data Analytics Project (JANUS)

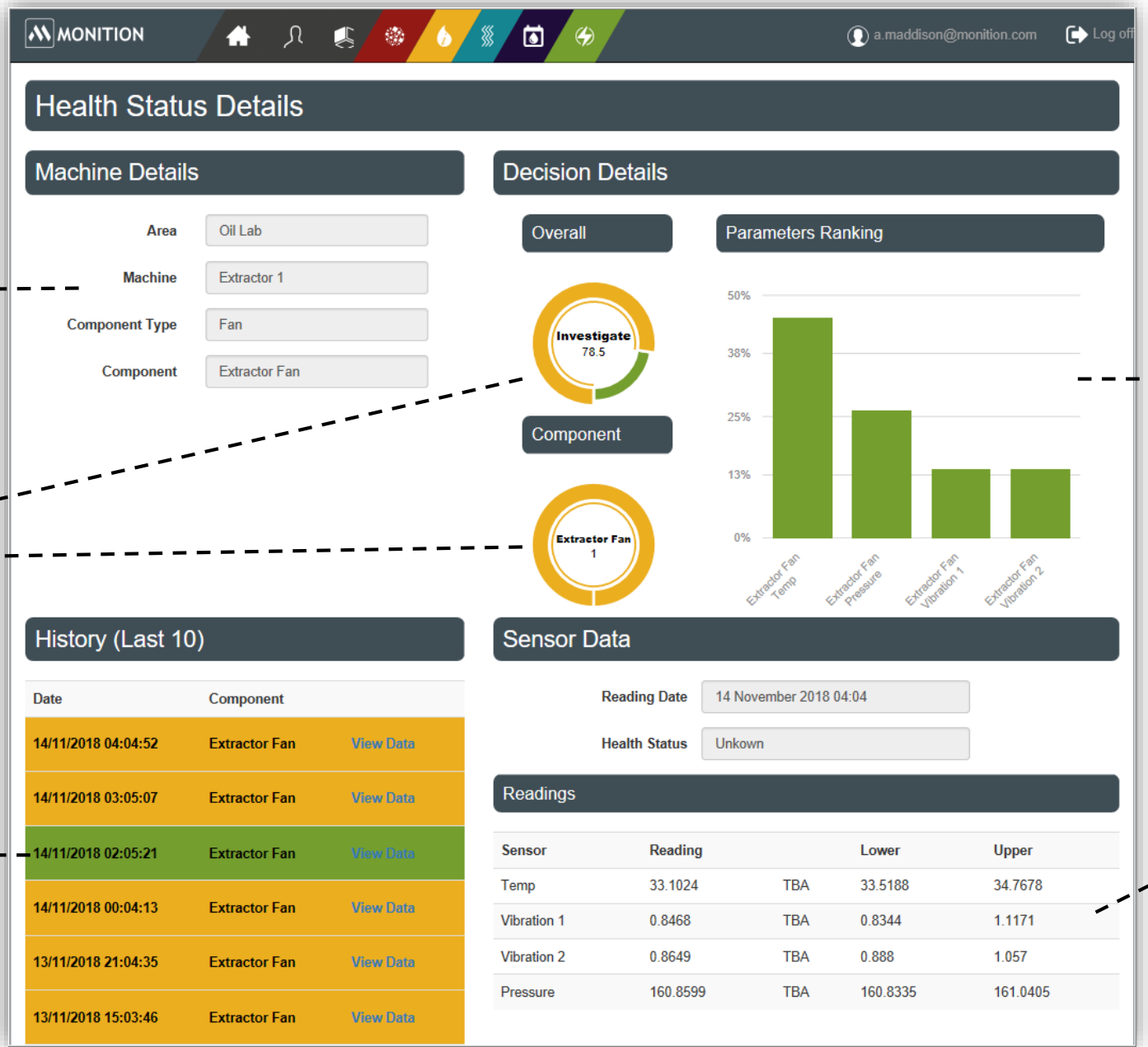
- **Aim :** Improvement of Maintenance Decision Making Using Machine Learning (ML) and Expert Systems

- **Functions Currently Active :**
  - Asset Diagnostics (Phase I)
  - Ranking of Desirable Maintenance Actions (Phase II)
  - Root Cause Analysis (RCA) (Phase II)
  - Analysis of Current vs. Desirable Health Performance (Phase II)



Monition i4.0 Intelligent Data Analytics Project (JANUS)

- **A Snapshot of the JANUS Dashboard**



Specifications of the system/asset (overview)

Decision making model outputs (Phase II)

ML- enabled data visualisation and diagnostics (Phase I)

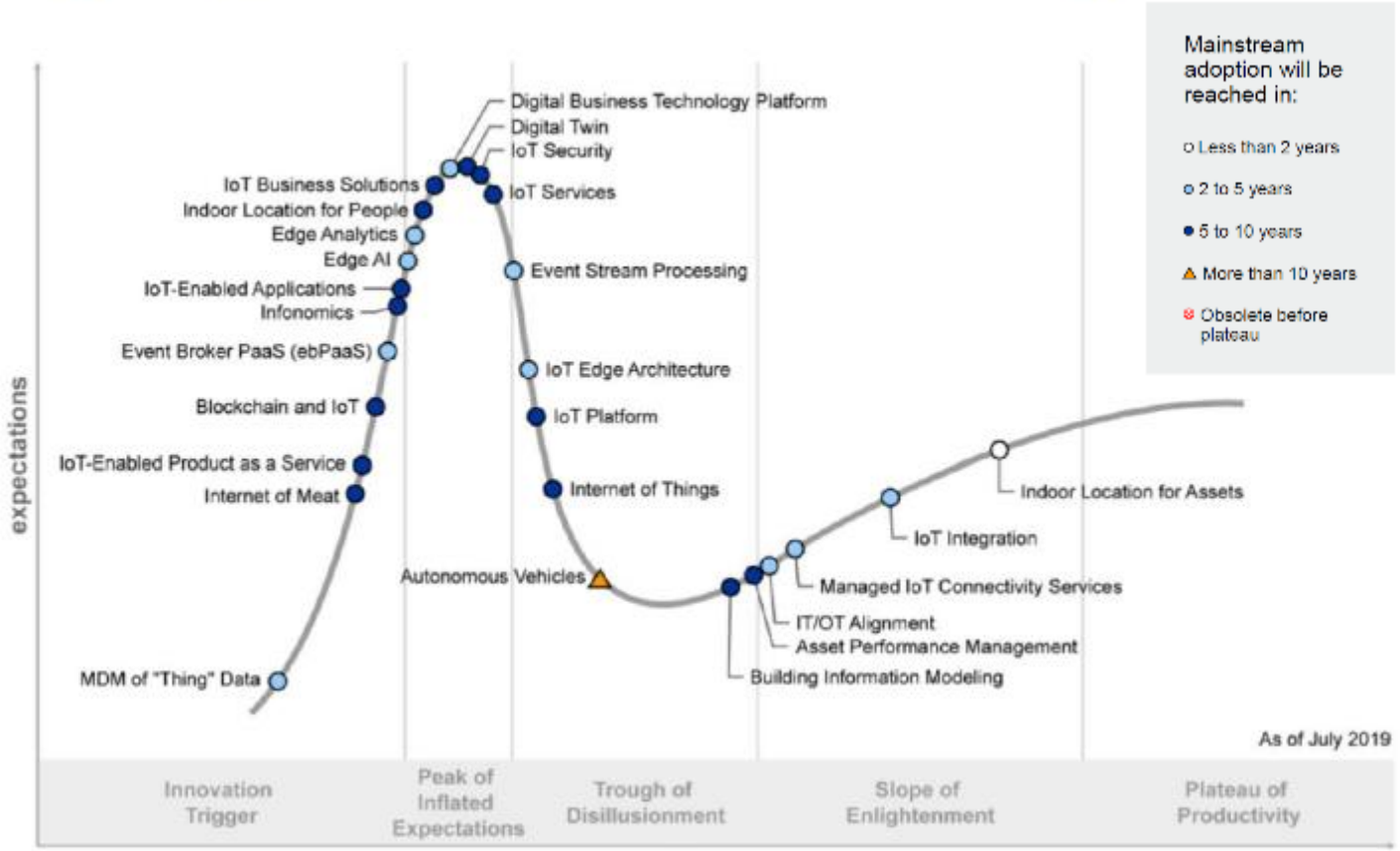
Parameters ranking for identification of the most likely cause(s)/contributor(s) of developing failure(s) (Phase II)

Sensor readings (overview)

https://www.youtube.com/watch?v=ystdF6jN7hc

IIoT Market Place

Hype Cycle for the Internet of Things, 2019



Magic Quadrant

Figure 1. Magic Quadrant for Industrial IoT Platforms

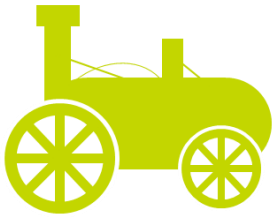
Source: Gartner (June 2019)

IIoT Market Place still lacks maturity .....

and there are no leaders

What's Industry 4.0?

1.0

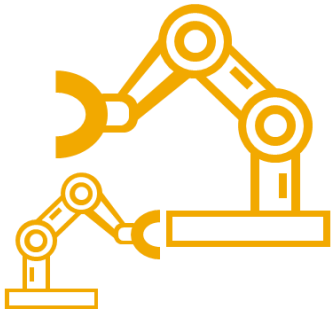


Mechanisation
Steam Engines
Water Power
New Manufacturing
Iron Production
Textile Industry
Mining and
Metallurgy
Machine Tools
Steam Factories

2.0

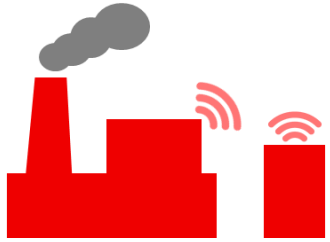
Technological
Electrification
Production Line
Mass Production
Globalisation
Engines & Turbines
Broad Adoption
of Telegraph, Gas,
Water Supply

3.0



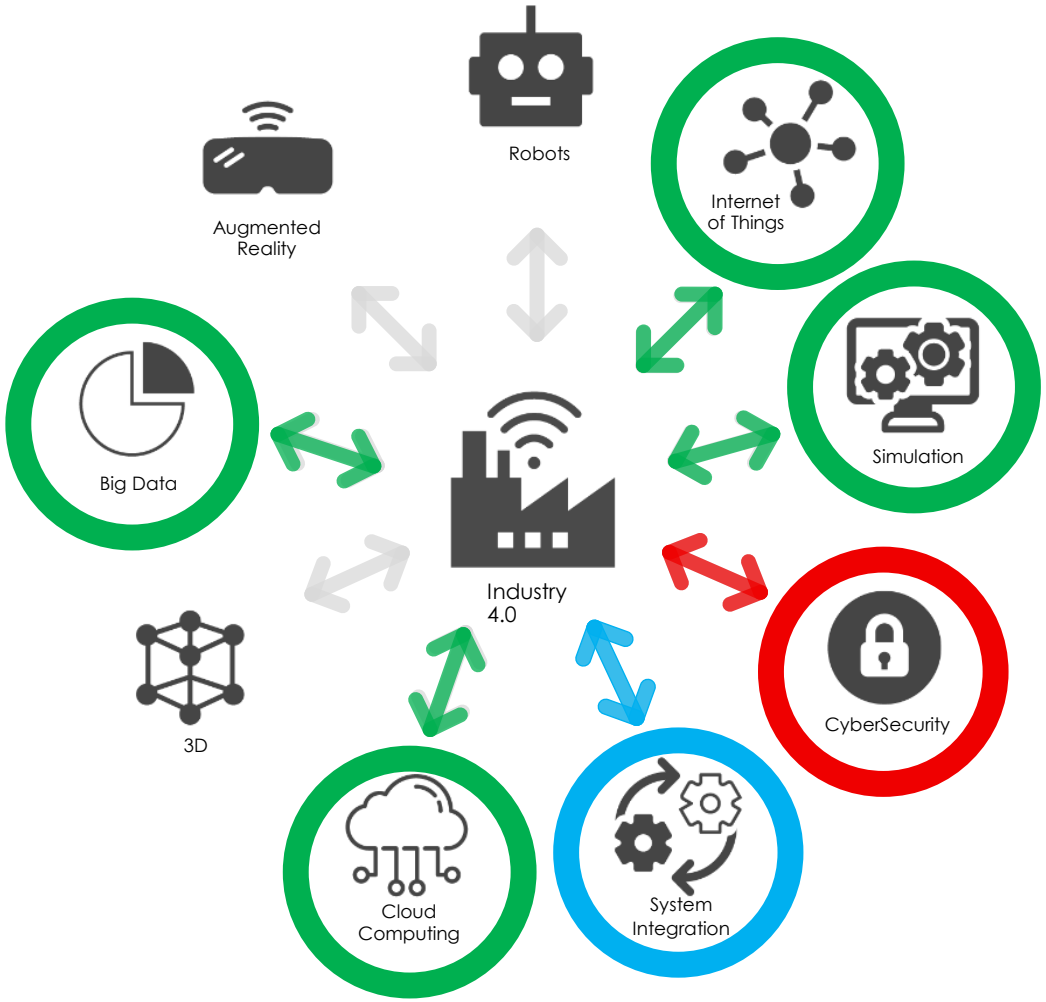
Computer/Internet
Digital
Manufacturing
PLC/Robotics
IT and OT
Digitisation
Automation
Electronic & Digital
Networks
Digital Machines

4.0

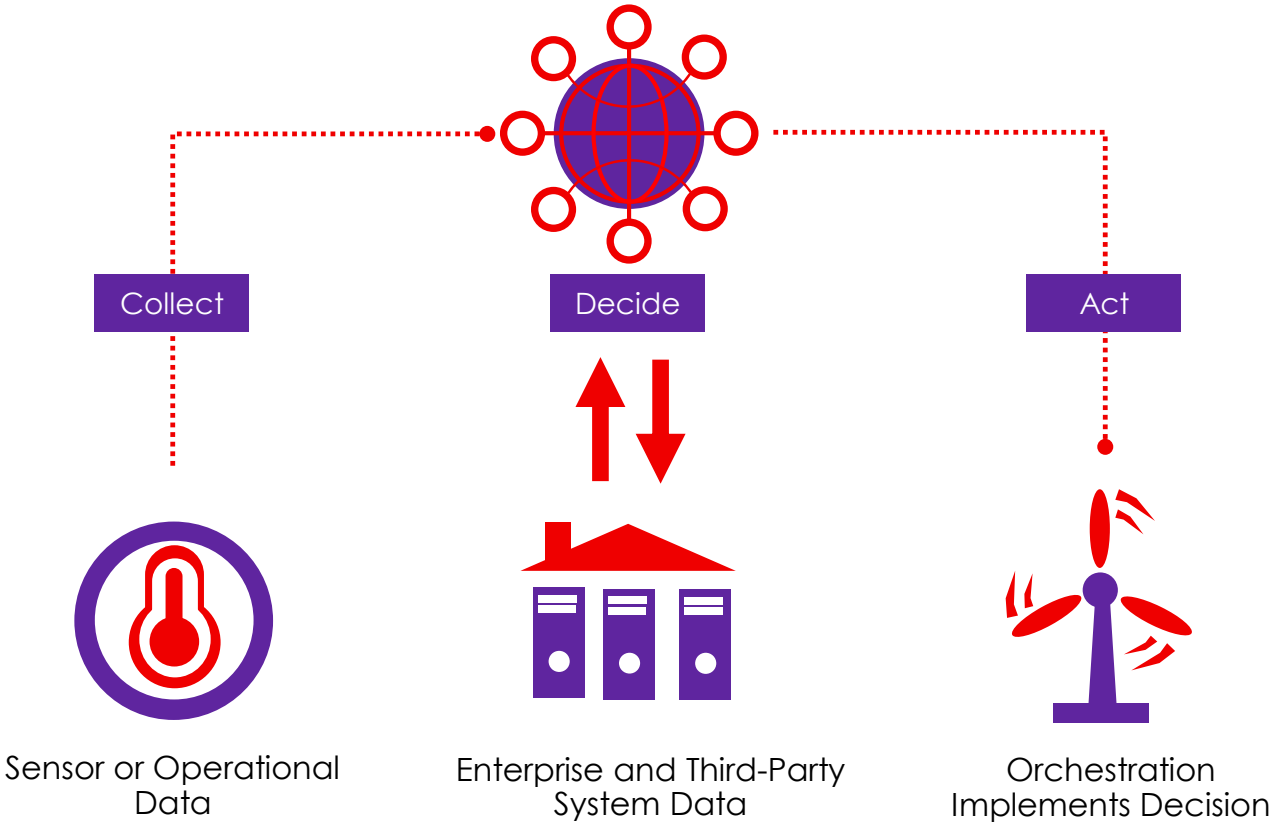


Convergence IT &
OT Autonomous
Machines
Advanced Robotics
Big Data/Analytics
Internet of Things
Cloud computing
Smart Factory
Machine Learning &
AI Cyber Physical
Systems

Industry 4.0: What's Involved



IoT Core Model: Collect – Decide - Act

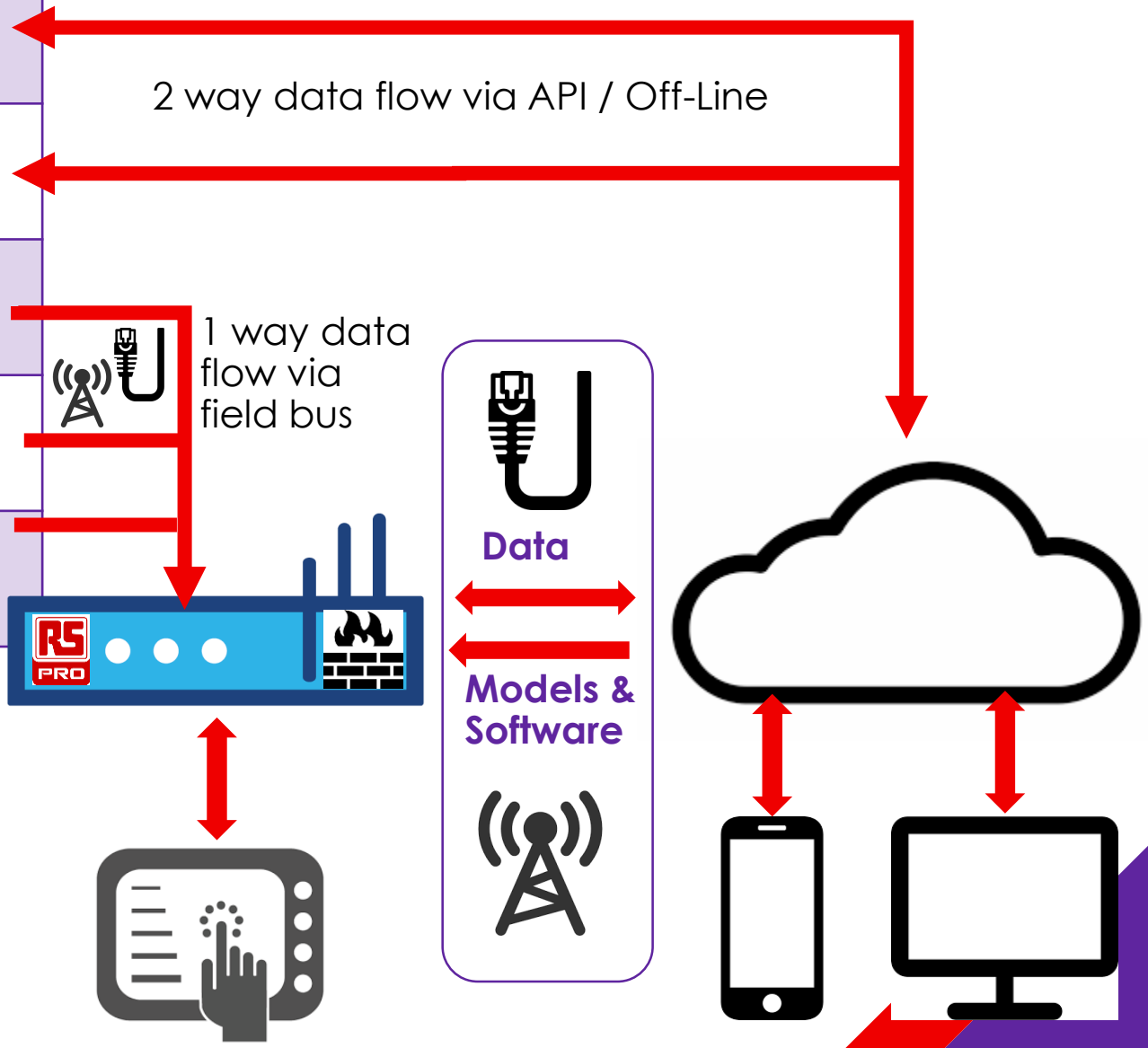


IIOT – Digital transformation – Take 1.

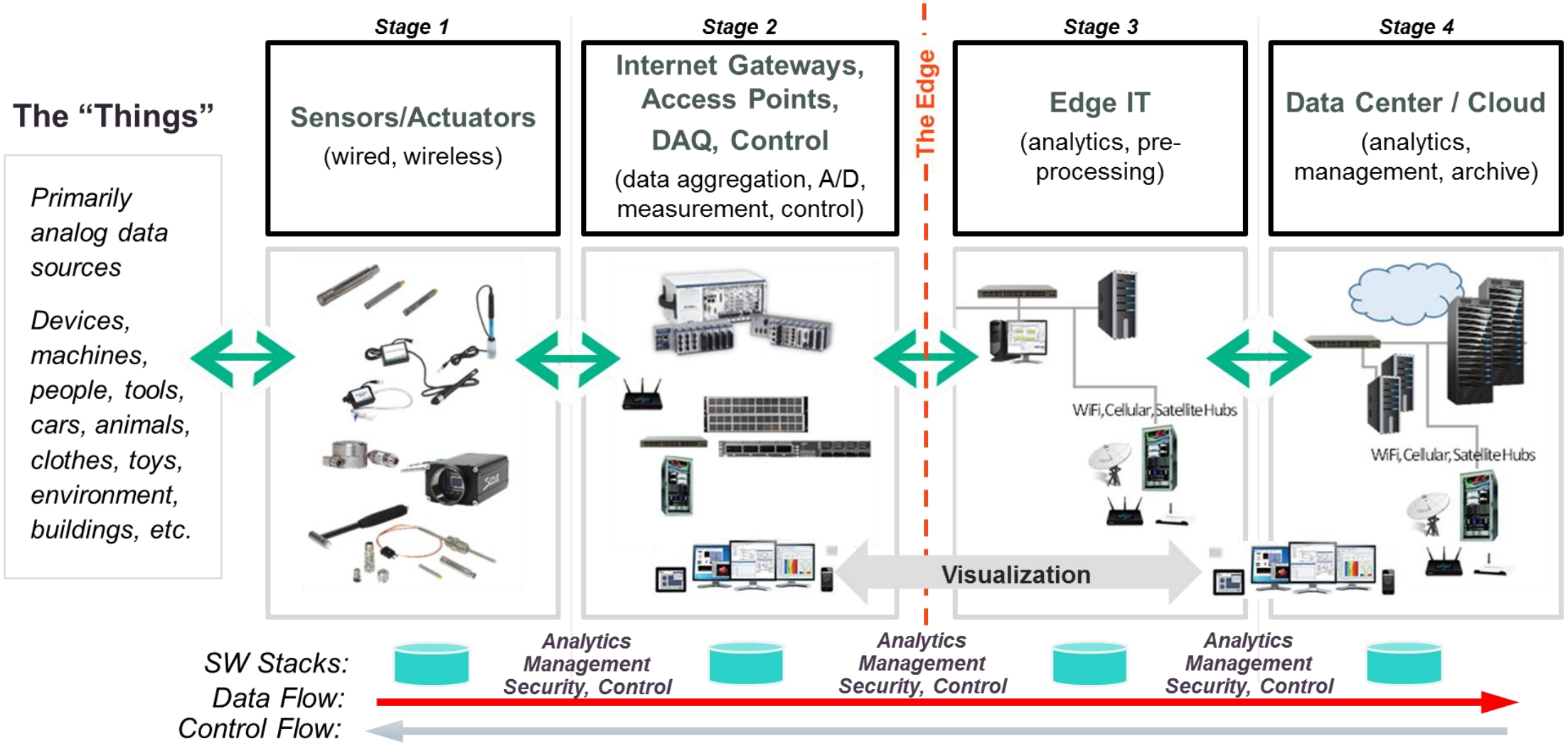
Free Hand

Simplified Edge & Cloud

Level 4	Enterprise	IT
Level 3	Management (MES, LIMS, WMS, CMMS)	IT
Level 2	Operations (SCADA, HMI, historian)	Field Bus
Level 1	Control (PLCs & Drives)	Field Bus
Level 0	Sensors & Actuators	Point to point comms to I/O

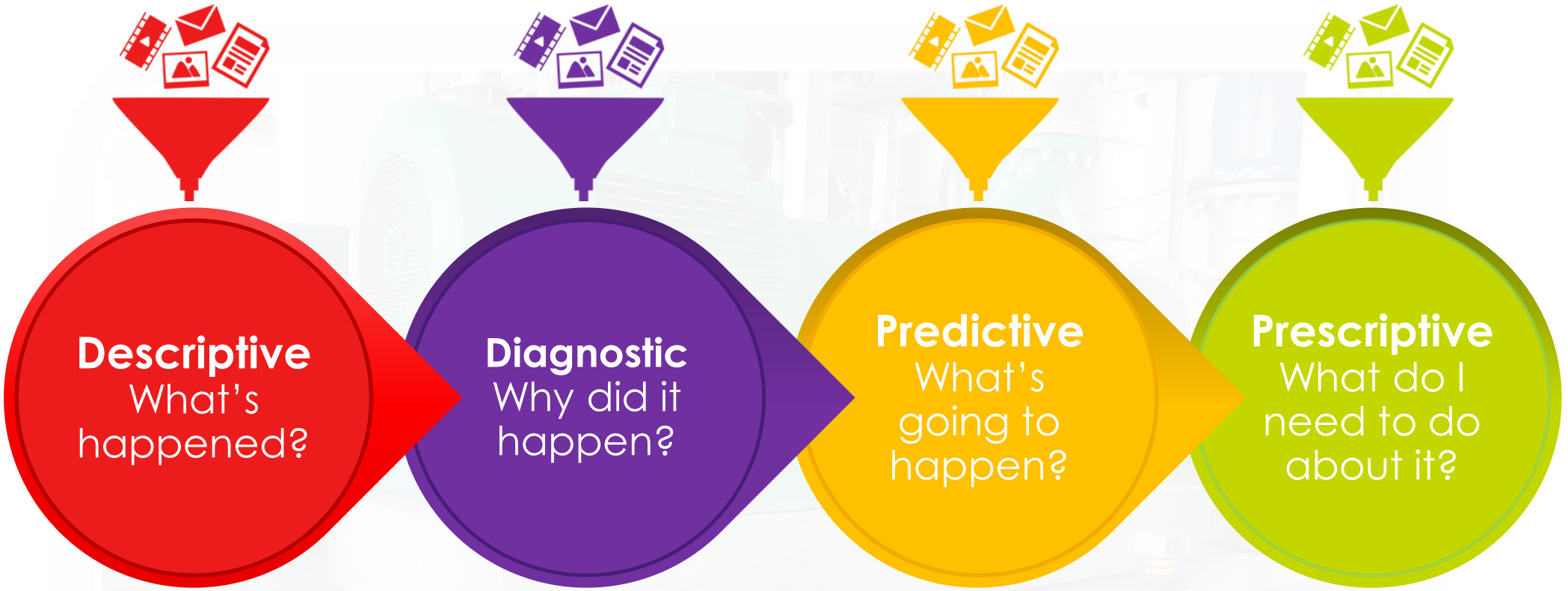


Typical Industrial IoT Implementation



Source: Industrial IoT Consortium

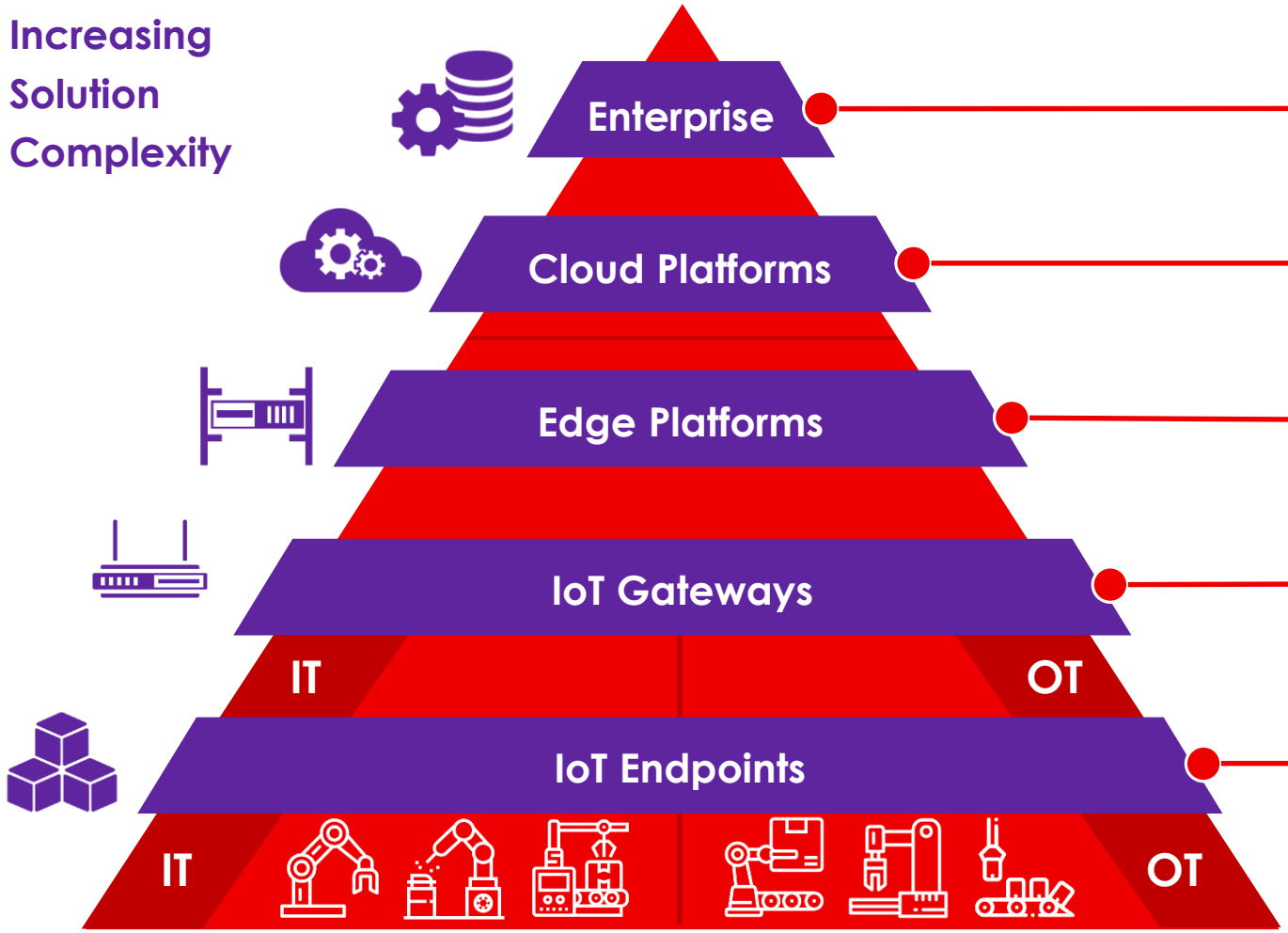
Turning Data into Insight and Insight into Action



- My pump is vibrating more than it should
- Because there is a blockage in the feed system and it's cavitating
- The bearing will seize in 10 hours
- Clear the blockage in the feed and inspect the pump for ancillary damage

The Technology Stack – The IT and OT Divide

Increasing Solution Complexity



Enterprise Applications

ERP CRM BM FSM MES… Data Center and / or Cloud

Cloud Platforms Public/Private/Hybrid/On-Premise

Standard Cloud Services and IoT Unique Cloud Services

Edge Platforms

Cloud Clone, Hybrid Cloud and Distributed IoT Services

IoT Gateways

Network and Protocol Translation, Data Aggregation…

IoT Endpoints

Connected Assets with Sensors, Compute and Communication

The Cloud (simplified!)

You do it

User Interfaces
e.g. mobile apps

Applications
e.g. data visualisation tools

Storage
i.e. databases

Operating Systems
e.g. Windows, Linux

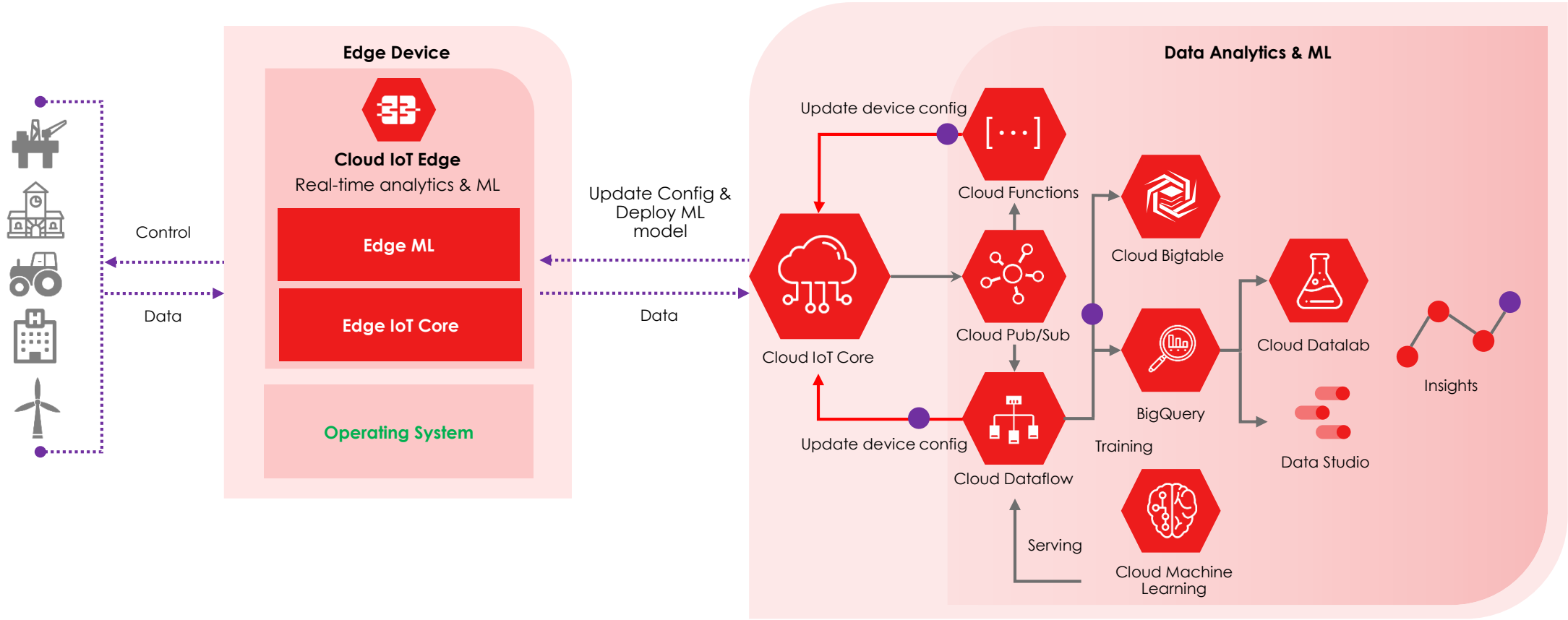
Infrastructure
i.e. physical kit + networking

Software provider

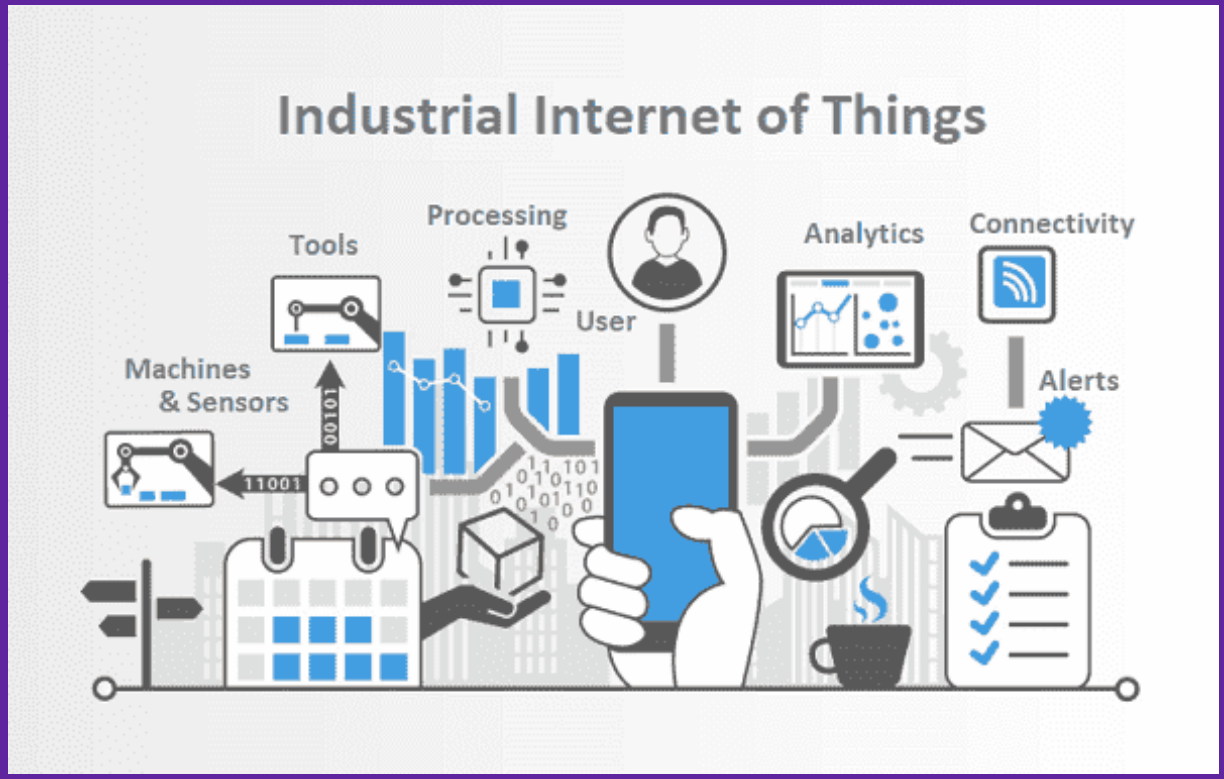
Software provider

AWS / Google/ Microsoft

Cloud architecture isn't easy to understand…
…it's even worse when it's not even in the cloud!



03 The Market



Wide estimates on size of the market – but all agree it's in massive growth

Industrial IoT Market by Device & Technology (Sensor, RFID, Industrial Robotics, DCS, Condition Monitoring, Smart Meter, Camera System, Networking Technology), Software (PLM, MES, SCADA), Vertical, and Geography - Global Forecast to 2023

DESCRIPTION | TABLE OF CONTENTS | METHODOLOGY

MARKETSANDMARKETS

Industrial IoT Market is expected to witness high growth during the forecast period. The industrial IoT market is expected was valued at USD 59.54 billion in 2017 and is expected to reach USD 91.40 billion by 2023, at a CAGR of 7.39% during the forecast period. The major factors driving the growth of the IIoT market include technological advancements in semiconductor and electronics devices, availability of automation solutions, improved data rates, and coverage of communication technologies; increasing use of cloud computing platform; growing adoption of IPv6; and support from governments worldwide pertaining to the adoption of IIoT solutions.

Industrial IoT Market Size is projected to surpass USD 771.72 billion by 2026

Published: Mar 6, 2019 1:43 p.m. ET

Mar 06, 2019 (Heraldkeeper via COMTEX) -- The 'Industrial IoT (IIoT) market' study published by Market Study Report, LLC, provides an in-depth analysis pertaining to potential drivers fueling this industry. The study also encompasses valuable insights about profitability prospects, market size, growth dynamics, and revenue estimation of the business vertical. The study further draws attention to the competitive backdrop of renowned market contenders including their product offerings and business strategies.

The global Industrial Internet of Things (IIoT) market is expected to reach a value of $922.62 billion by 2025, according to a Million Insights report released on Monday. This growth is due to the worldwide rise in IoT technology development and implementation in the past few years.

Artificial Intelligence devices in manufacturing to hit 15 million by 2024

Posted on 25 Sep 2019 by Jonny Williamson

The total installed base of AI-enabled devices in industrial manufacturing is forecast to reach 15.4 million within five years, with a CAGR of 64.8% from 2019 to 2024.

Industrial IoT Market Size Worth $949.42 Billion By 2025 | CAGR: 29.4%

June 2019 | Report Format: Electronic (PDF)

The global industrial internet of things market size is expected to reach USD 949.42 billion by 2025, according to a ne report by Grand View Research, Inc. It is projected to expand at a CAGR of 29.4% during the forecast period. Rising demand for machine-to-machine systems, the need to contextualize the Operation Technology (OT) data, and preference for predictive maintenance are the factors anticipated to drive the Industrial IoT market growth.

Similar picture with market research conducted by RS China

RS Situation and Scope

RS Components Objectives

- Develop a services package based around RS cloud to include mobile Computerized Maintenance Management System (CMMS), stock management, and condition-based monitoring (CBM) to help digital factories run optimally.
- Become design authority/influencer on the implementation of the smart factory environment.
- Deepen RS's understanding of the competitive environment and profitable opportunities in China

Scope

- Target Customers: Discrete and process manufacturers, machine builders
- Markets Segments: CMMS, condition monitoring solutions, smart factory design consultants and SIs
- Geographic Scope: Mainland China
- Execution Timeline: 3 weeks, from September 16 to October 4

IoT ONE Deliverables

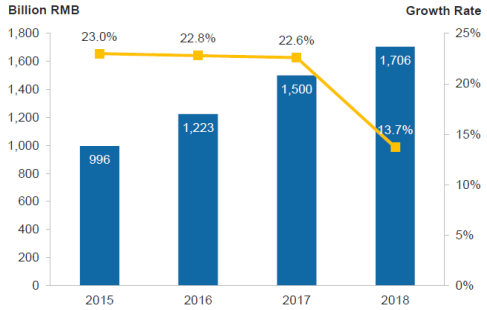
IoT ONE will support RS Components in assessing three areas to support confident strategy development.

1. Landscape Mapping: Assess the competitive landscape of the mobile CMMS and condition monitoring markets in China.
2. Business Model Analysis: Evaluate the business/operation models of players along the smart factory design and system integration value chain.
3. Economics Analysis: Evaluate the economics of smart factory design consultancy in China, including pain points, value perception, service areas, pricing levels, and resourci… Assess differences by end customer industry type and ownership structu…

China Smart Factory Market Overview

China's investment in factory technology remains robust despite the trade war but may trend towards domestic suppliers.

Factory Technology Investment Scale and Growth



Ranking of Advanced Manufacturing Technology Focus by Region

Advanced Manufacturing Technology	China	USA	Europe
Predictive analysis	1	1	4
Smart factory IoT	2	4	1
High performance computing	3	6	7
Advanced materials	4	3	5
Digital design, simulation and integration	5	5	3
AR (quality, training, and output knowledge)	6	10	8
Smart connected products IoT	7	2	2
Advanced robotics	8	7	6
AR (customer service and experience)	9	11	11
Open source design / customer direct input	10	9	10
Additive manufacturing (3D printing)	11	8	9

- Technology investment in Chinese factories reached 1,706 billion RMB in 2018 and continues to grow at a healthy 13.7% despite a sharp decline relative to prior years. The downward pressure was likely caused by investment concerns related to the US trade war.
- A 2018 survey by AskCI of factory managers regarding the importance of advanced manufacturing technologies identified predictive analytics and smart factory IoT solutions as the top priorities in China.

…for domestic, or non-…e Council.

3

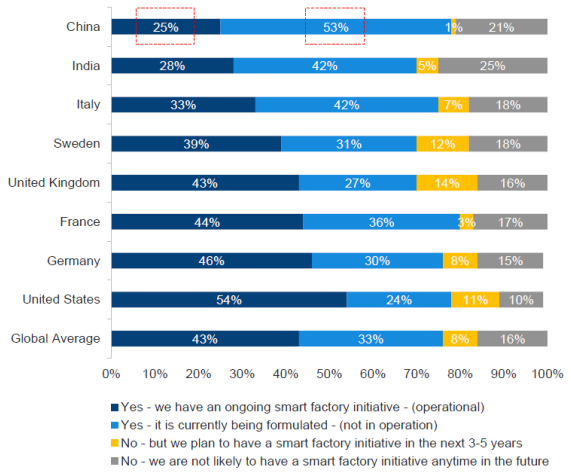
China Competitive Landscape Mapping

IoT ONE | 2019-10-10

China Smart Factory Market Overview

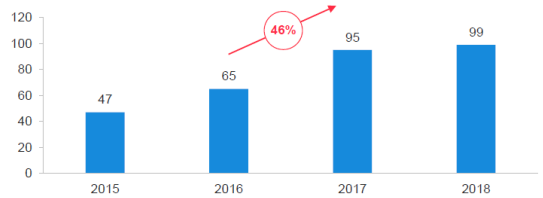
Upgrading factories is a national-level priority tied to China's goal of sustaining manufacturing leadership as labor costs rise.

Smart Factory Implementation Status by Country (2016)



Source: Capgemini, Ministry of Industry and Information Technology of PRC

China Nationally Recognized Smart Factory Pilot Projects



- In 2016, China reported the lowest proportion of companies with ongoing smart factory initiatives at 25%.
- Yet Chinese factories have the strongest intent to formulate a smart factory initiative at 53%.
- From 2016 to 2017 the number of nationally recognized smart factory pilots jumped by 46% in China.
- In 2019 Q1 the government launched policy initiatives that will "move forward China's smart factory development by 5 years" according to the CEO of Black Lake Technologies.

4

The Customer's Challenge – Cyber Security

In partnership with: VAUBAN GROUP

MAKE uk The Manufacturers' Organisation

UK manufacturers "woefully unprepared" against cyberattack

Posted on 10 Sep 2019 by Jonny Williamson

More than half of manufacturers have been the victim of cybercrime, and a third of those have suffered some financial loss or disruption to business as a result, according to a major new report.

The manufacturing sector is the fifth most targeted for cyberattack in 2019, behind government systems and finance. Worryingly, however, industrial businesses remain among the least protected against cybercrime in Britain.

27% of manufacturers told us they do not have a risk register or mitigation plan limit the threat

33% do not provide awareness briefs or formal training to their employees

55% do not have insurance to cover loss due to cyber-attack

41% do not have a nominated lead for cyber security at board level

49% do not monitor cyber security performance through key business performance indicators

Source: Make UK Cyber Security survey, May 2019


Questions?

irwinmitchell

Go Fourth

irwinmitchell

Get Yourself Connected

By 2025, there'll be 26 billion connected devices on the planet – more than three devices on average for every single person

2.5 quintillion bytes of data is being produced every day

Manufacturers have never had so much accurate information about their operations as they do today

But with volume comes risk…

irwinmitchell

Defining Industrial Data

Structured data
Data organised into a specific formatted storage system, such as a database or spreadsheet

Unstructured data
Data that isn’t stored in a predefined format or data model, such as office documents, PDFs, CADs, etc

Information classification
The grading of data on its sensitivity or impact to the business if lost or mishandled

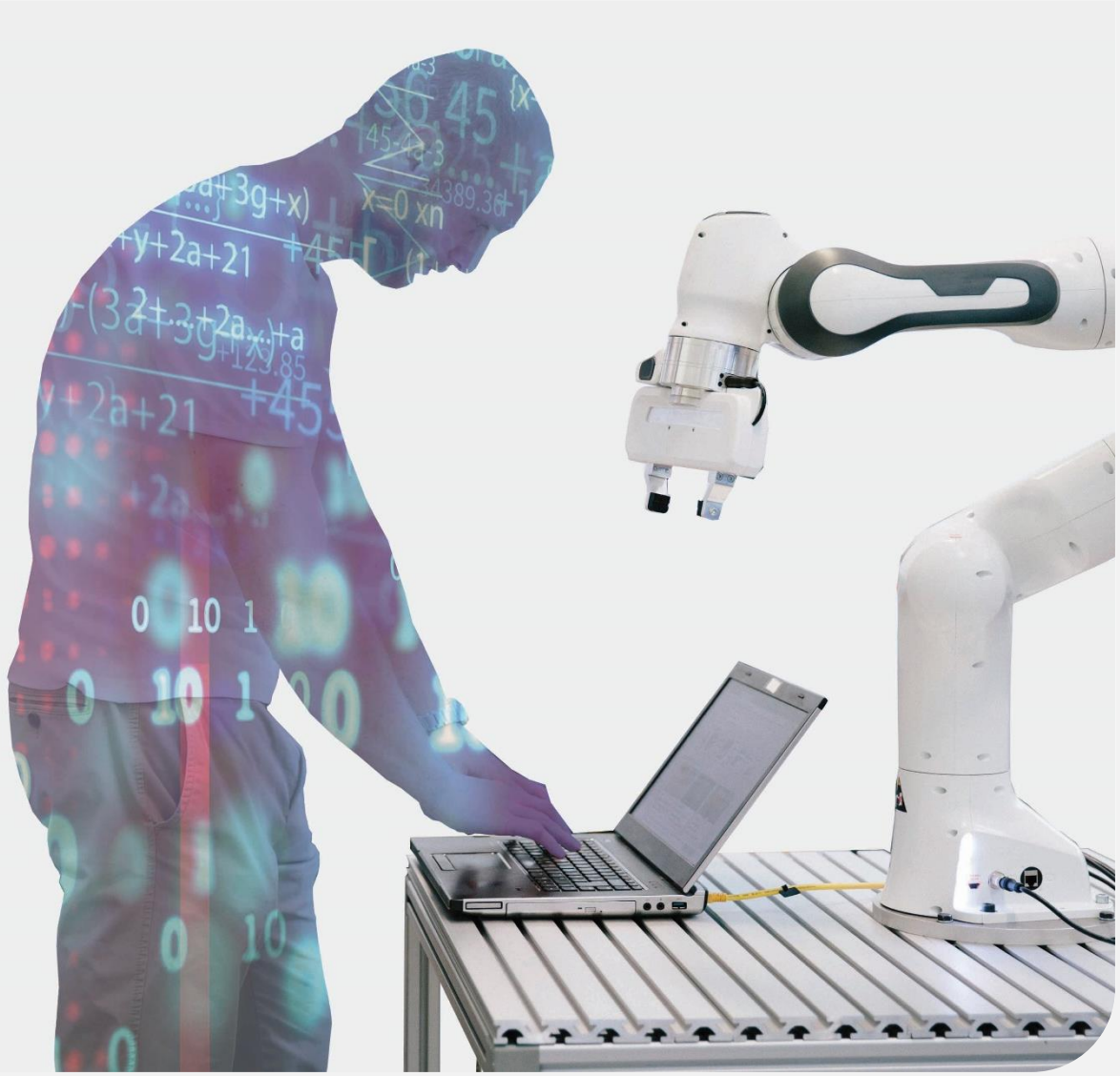
Data and Employment Law

Employee data collection in manufacturing

- Workstation performance data
- CCTV
- Telematic tracking
- Screen monitoring software

Potential employment law issues

- GDPR breaches
- Subject Access Requests (SAR)
- Discrimination
- Disciplinary procedures / dismissal
- Liability for acts of employees



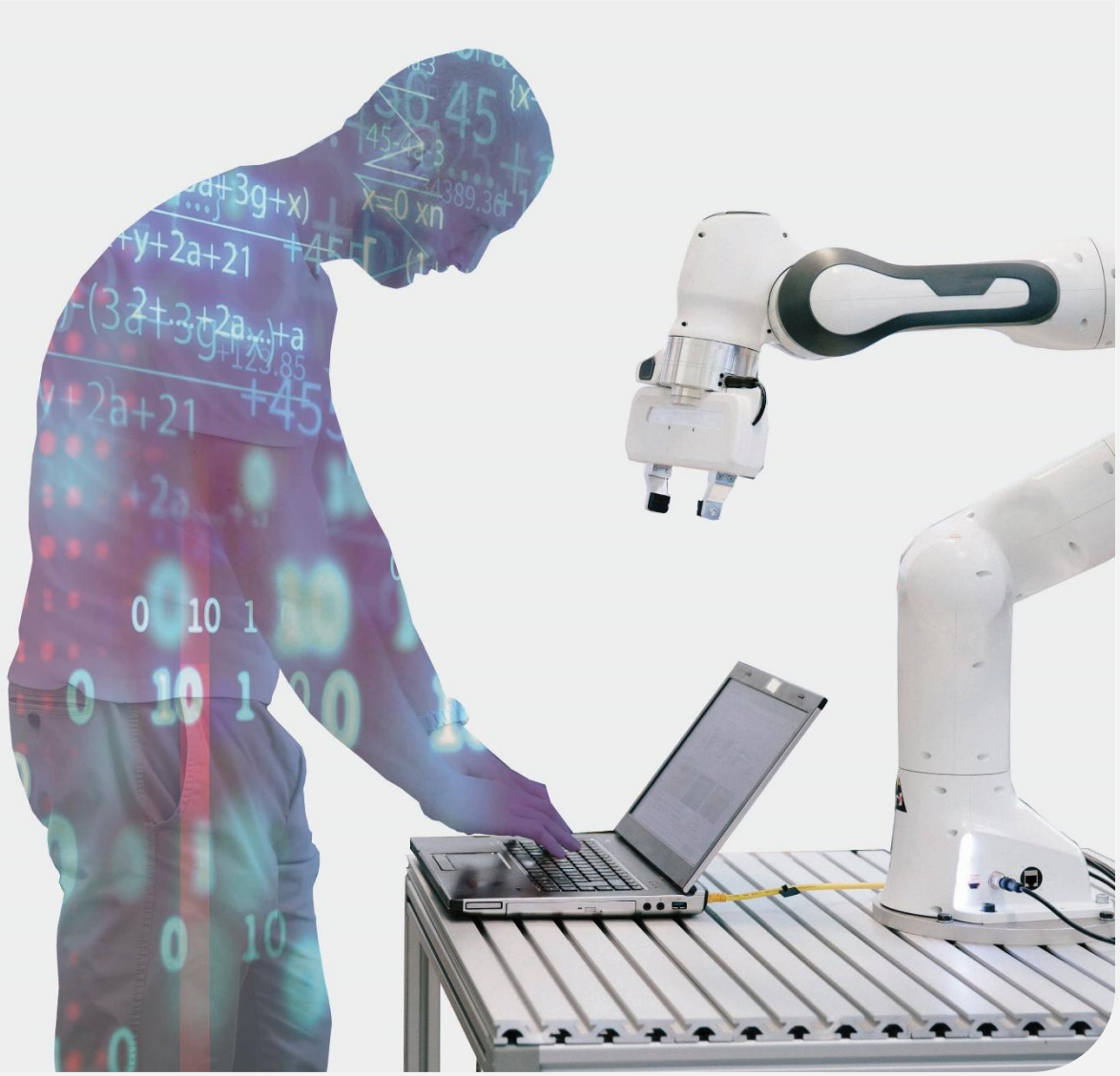
irwinmitchell

Best Practice Guide To Data Collection Notification

1. **Complete a Data Protection Impact Assessment**, a form of risk assessment, to make sure you're recording the data proportionately.

2. When you're satisfied this is proportionate, **assess if the information is transparent enough**. Draw up an Employee Monitoring Policy.

3. **Provide a privacy notice**, explaining to the staff again what you intend to do and how the data is collected.



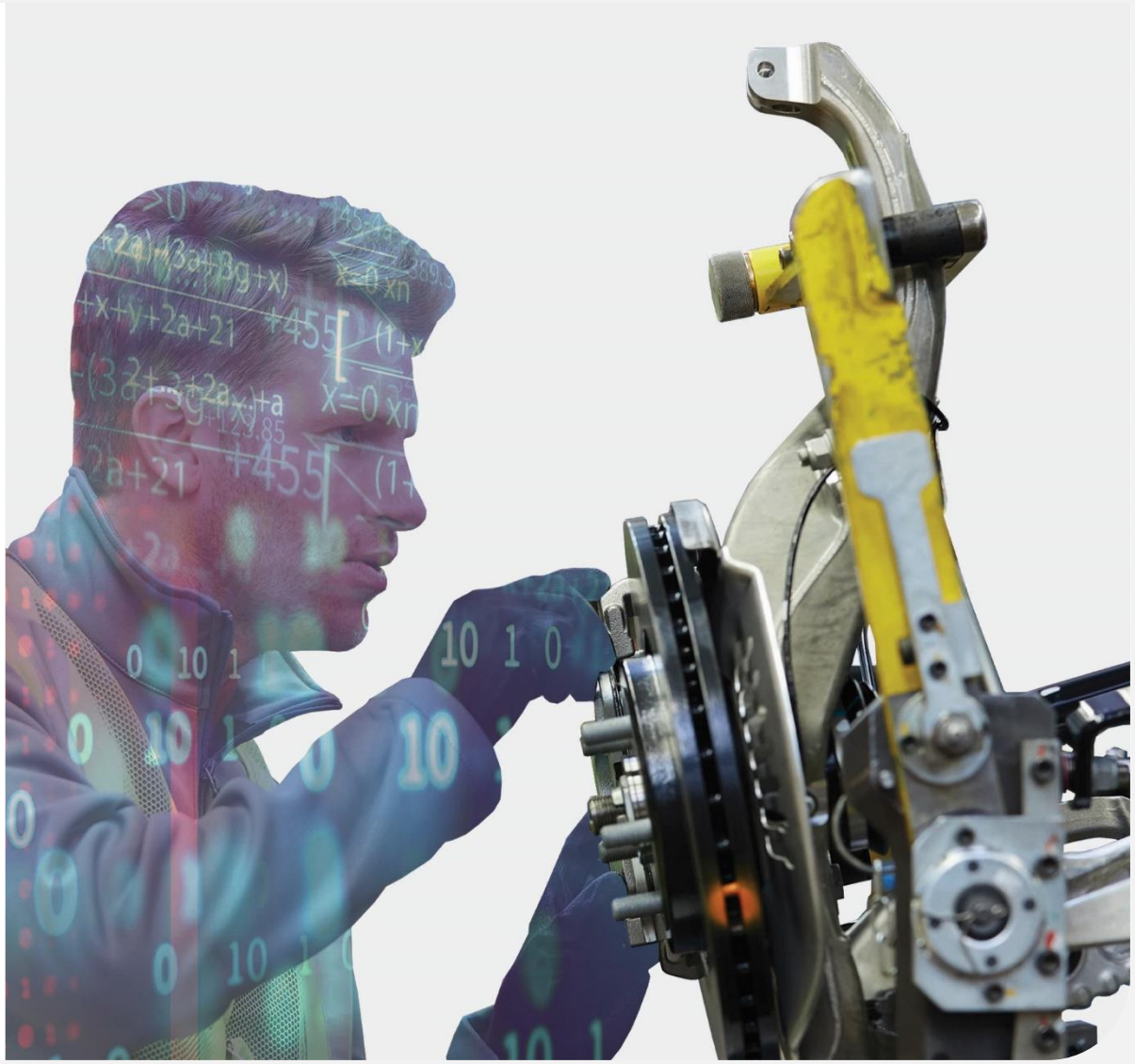
irwinmitchell

Finding Value In Harnessing Data

£455bn
– What faster adoption of ‘industrial digital technologies’ could be worth for UK manufacturing over the next decade

Advantages of digital records vs. paper ones
- Instant visibility across the company
- Multiple users able to see changes simultaneously
- Harder for information to be lost
- Access can be authorised

Technology in digitised factories
- Workstation touch screens
- Tablets
- Virtual reality headsets
- ‘Smart gloves’



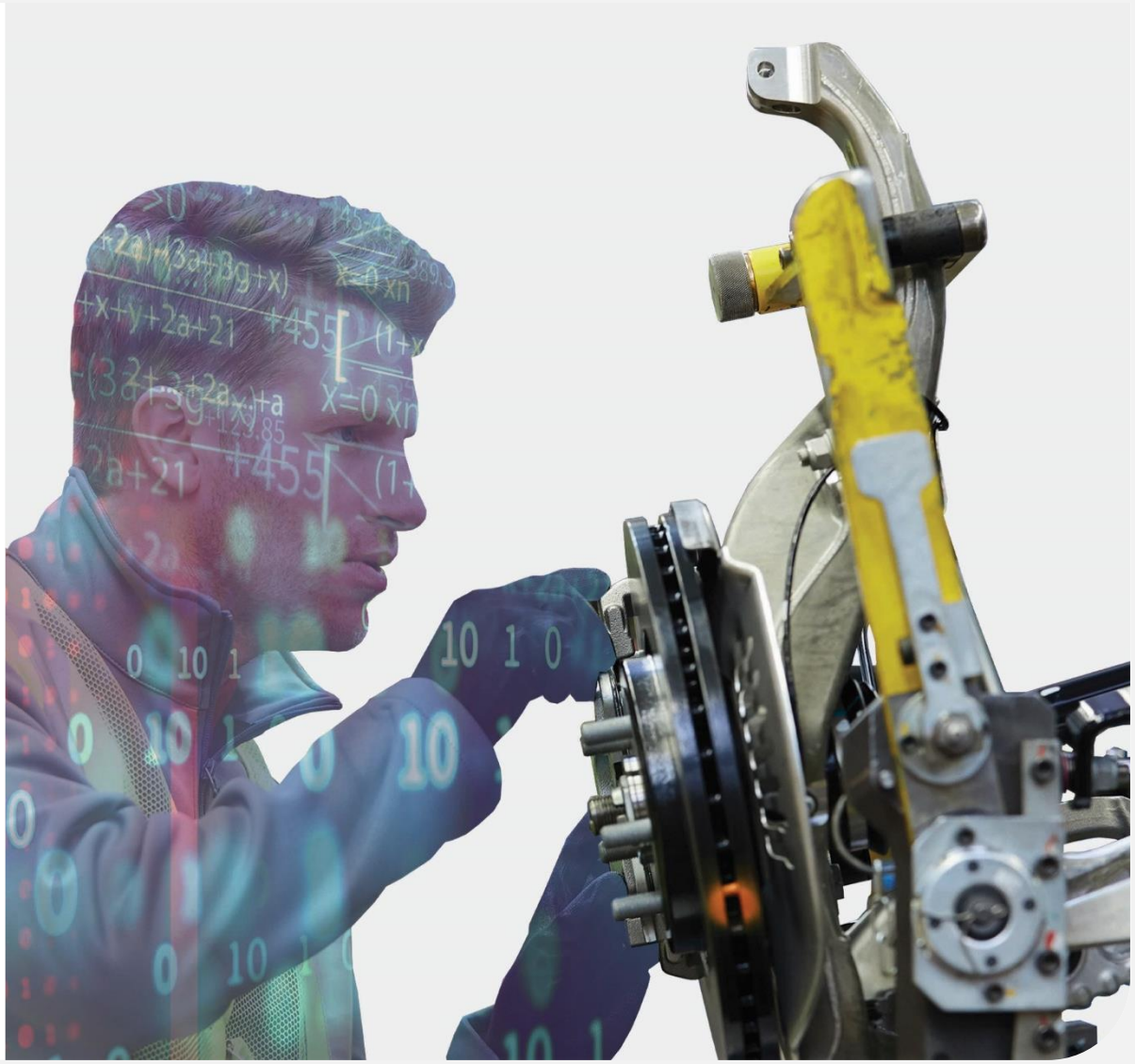
irwinmitchell

Sharing Data In Supply Chains

Data sharing has improved customer-supplier relationships

Suppliers have to buy technology and tools to be in a connected supply chain and share their data

Demand forecasting means companies can respond more quickly to changing trends



irwinmitchell

Cyber Security in Manufacturing & Engineering

January 2020

Graham Thomson

Chief Information Security Officer

irwinmitchell

Agenda

Types of cyber-attack

The key risks

The impact

The solution

The key defences

Types of cyber-attack

Learn more, search for:

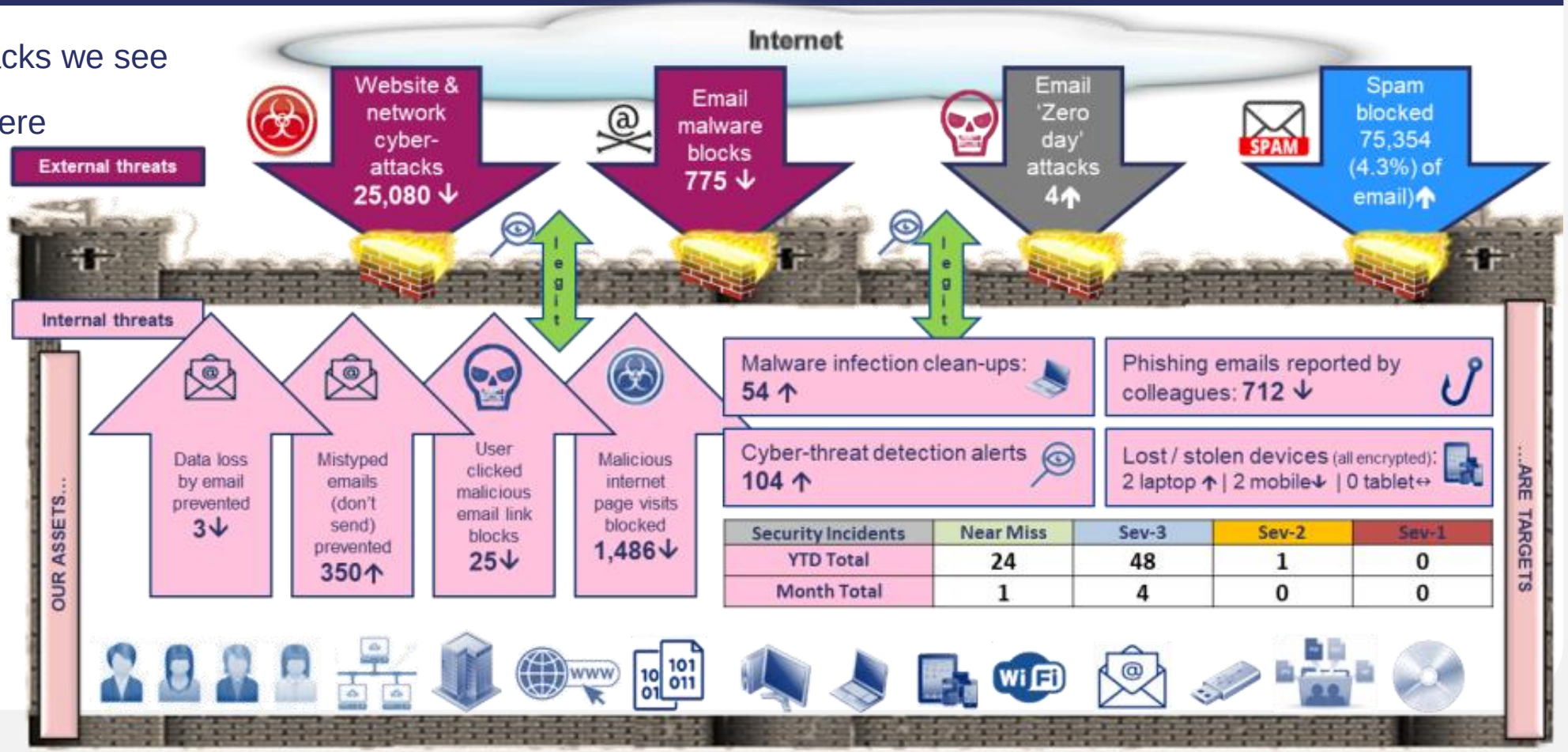
- *ncsc common cyber attacks*

"Attacks on industrial control systems have been occurring since the late 1990s, but they didn't become mainstream until 2010, when Stuxnet malware was discovered. That changed everything"

FireEye, ICS Consultant

Real-world situational cyber-awareness

- Typical monthly attacks we see
- It's cyber-war out there

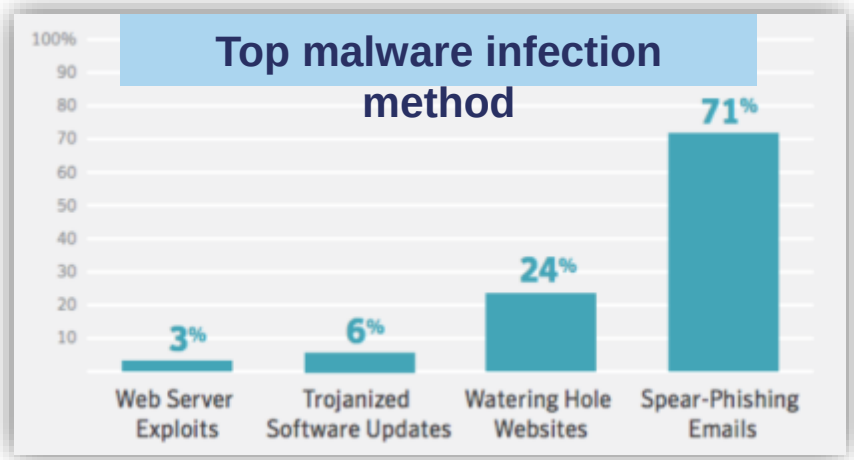


Security Incidents	Near Miss	Sev-3	Sev-2	Sev-1
YTD Total	24	48	1	0
Month Total	1	4	0	0

The key risks

Phishing: the #1 Cybersecurity risk

- Phishing is basically it's a confidence trick
- It's social engineering
- Email is the choice tool, but can use any form of communication
    - Impersonation attacks (CEO send payment frauds)
    - Malicious attachments (malware)
    - Malicious web links (malware or password theft)



Source: Symantec

> ***1 in 131 of all emails contains malware***
> *Symantec*

> ***Two-thirds of all malware is installed via email attachments***
> *Verizon*

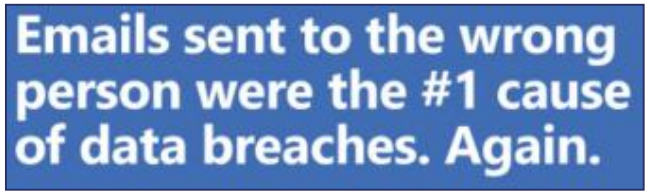
The key risks

Other top cybersecurity risks

- **#2 = Password risks**
  - weak / reused / compromise elsewhere
  - remote access compromise
  - website login stuffing (including ICS exposed to the internet)

- **#3 = Data loss**
  - mistyped / misaddressed emails (15% of all personal data breaches)
  - lost /stolen IT devices
  - insider data theft

- **Others include:**
  - malware infections (ransomware, ICS takeover, data stealing, etc.)
  - hacking internet facing assets (websites, IoT, ICS, etc.)
  - supplier risk (careless with your data, can access your network, compromised IT equipment)



The impact

- **Financial impact**: direct losses of money, weakened sales if competitive edge is lost
- **Operational impact**: factory downtime
- **Reputational impact**: global media coverage, IP theft can lead to a flood of counterfeit products
- **Growing regulations**
  - DPA 2018: tougher fines for data breaches
  - Up to £17m or 4% of turnover
- Despite this, ICS/OT cyber-protection levels are still low

DaimlerChrysler victim of a cyberattack from the Zotob worm in 2005

In 2005 in the USA, the **Zotob worm** was used to attack various industrial infrastructures. Thirteen factories were affected and had to completely stop operations for 1 hour. This led to 14 million dollars in losses for DaimlerChrysler.

Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies

Symantec's artificial-intelligence-based Targeted Attack Analytics uncovers new wide-ranging espionage operation.

Researchers Found They Could Hack Entire Wind Farms

Hackers built proof-of-concept malware that can spread from turbine to turbine to paralyze or damage them.

The solution

1/ Have a strategy and someone to own it

2/ Pick an industry standard (some are free)

NIST Cybersecurity Framework Manufacturing Profile
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923839

3/ Deliver & maintain it

4/ Measure it (what gets measured gets done)

www.cisecurity.org/controls
Very detailed

www.ncsc.gov.uk/guidance/10-steps-cyber-security
Simple

www.nist.gov/cyberframework
Combines standards

www.iso.org/isoiec-27001-information-security.html
£££ - and not always clear

Key defences against the digital dark arts

#1 People

- Develop the human firewall (secure culture)
- Annual all staff training & awareness
- Regular phishing testing

#2 Process

- Have an infosec policy and minimum standards
- Method for colleagues to contact infosec
- Use cyber threat intelligence
  - Paid: SecurityScorecard, BitSight
  - Free: NCSC's CiSP, HaveIbeenpwned

#3 Technology

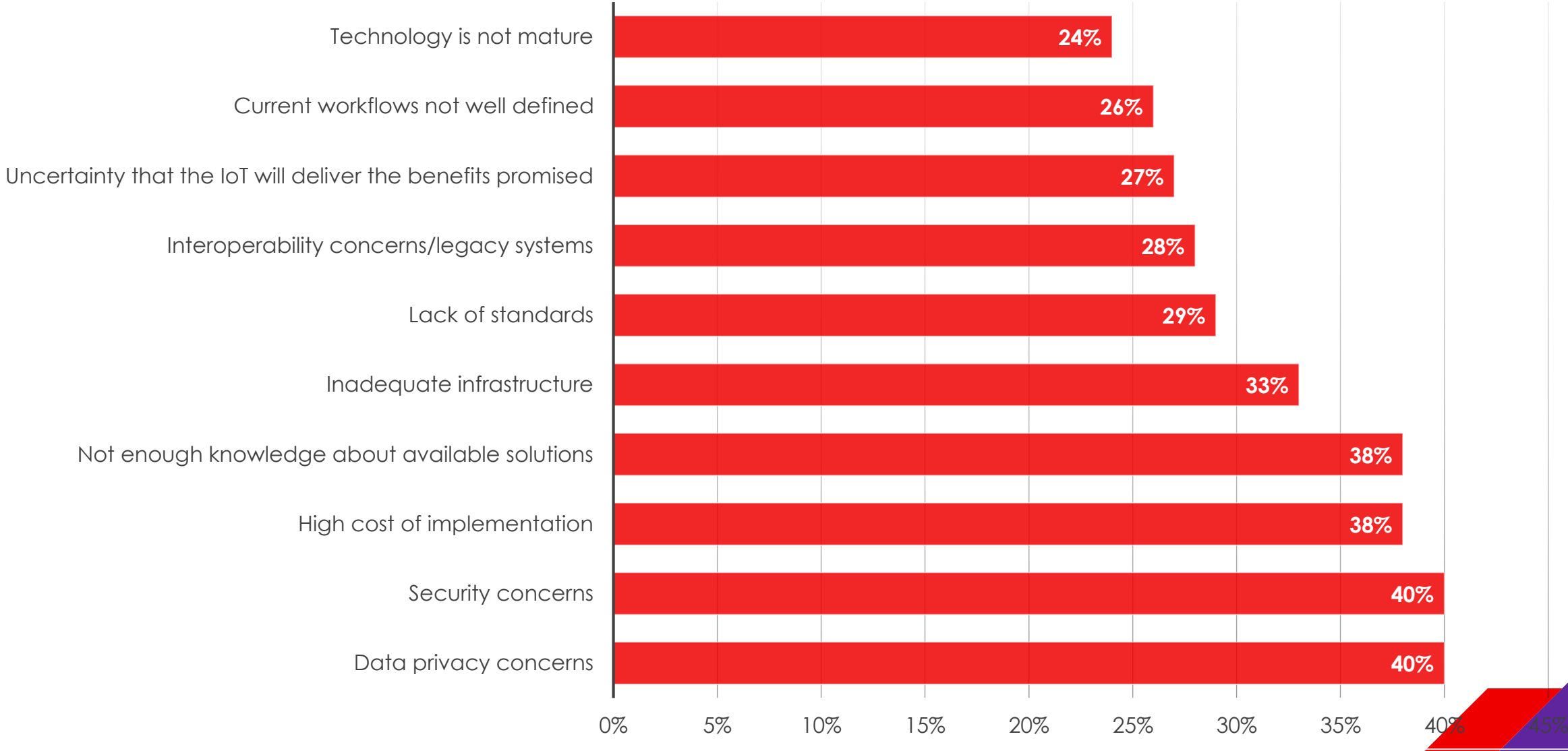
- Remove local admin rights from normal user accounts (mitigates 85% of risk)
- Use two-factor authentication for ALL network and email remote access
- Have a strong password policy
- Scan your public facing IP network – find out what's exposed to the internet
- Block dodgy emails with Secure Email Gateways (email filter)
- Clearly mark an email is from an external sender ("THIS IS NOT FROM US")
- Block dodgy websites with Secure Web Gateways (web filter)
- Block malware with endpoint security (EDR with AI is better than antivirus)
- Prevent data loss (laptop, mobile & USB encryption, mistyped email protection)
- Activate antivirus and Intrusion Prevention (IPS) on your firewalls

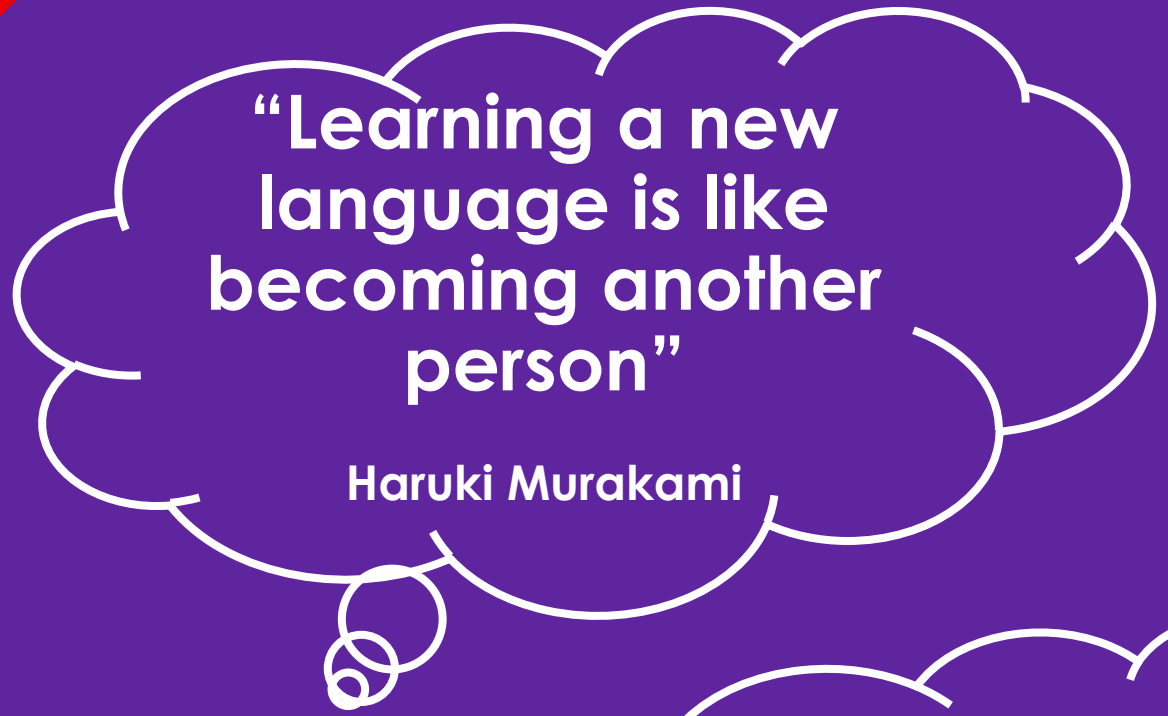
The future is AI and machine learning - automated cyber threat detection

04 Lessons Learnt from IIoT Journey

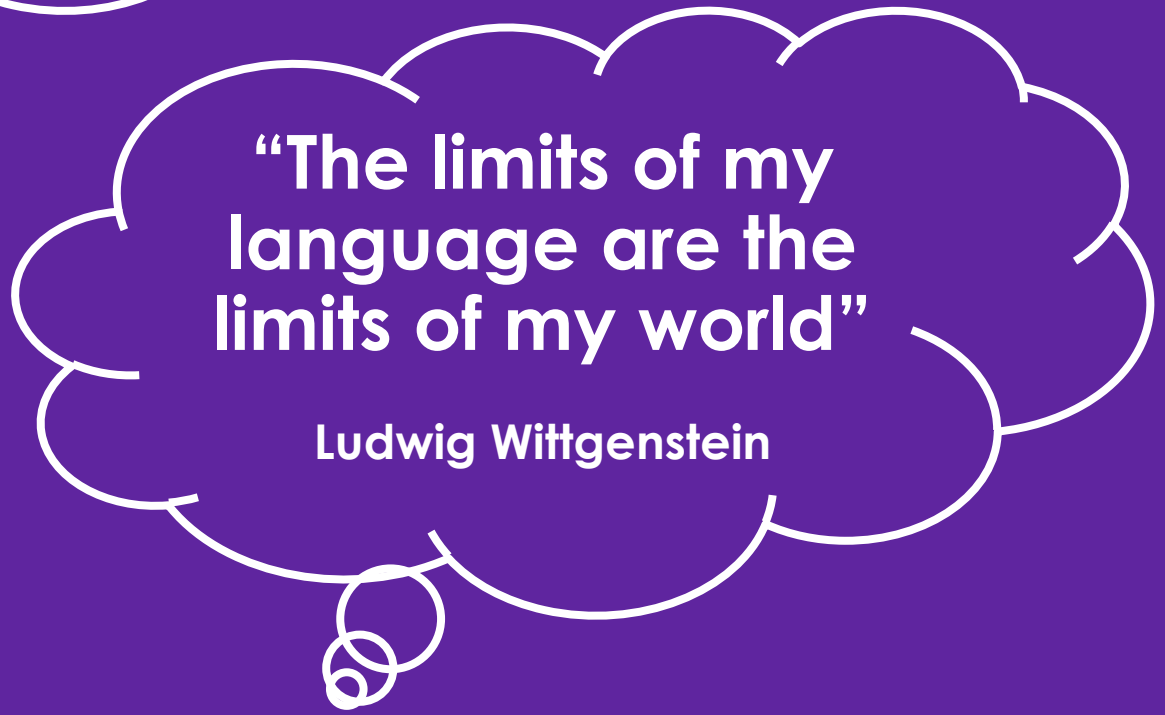
Key barriers to IIoT adoption – that we need to address

Consistent between studies – data from https://www.iotworldtoday.com/2016/04/20/top-10-reasons-people-aren-t-embracing-iot/




“Learning a new language is like becoming another person”
Haruki Murakami


“A new language is a new life”
Persian Proverb


“The limits of my language are the limits of my world”
Ludwig Wittgenstein

Embrace FAILing because....

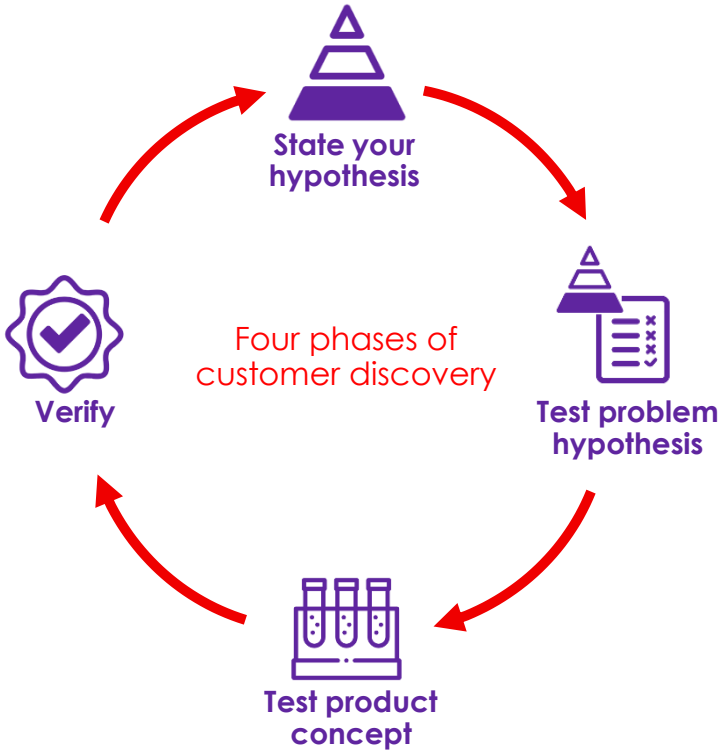
First Attempt Is Learning

Fail Quickly
Fail Cheaply
Fail Early
Fail Often
Fail Safely

The (original) problem we tried to solve

What	Early detection of failure and significant efficiency loss in small electric motors at an installed cost per motor of <£100 combined with recommended actions to be taken
Where	Distributed installations of 100+ motors in factory and warehousing environments with limited line of sight connectivity for wireless communication
When	Continuous sensing and analysis in near real-time (within 5 minutes of the fault)
How	Through the sensing or harvesting of a suitable leading indicator and analysis either locally, at the edge or in the cloud

Customer Discovery Conversations

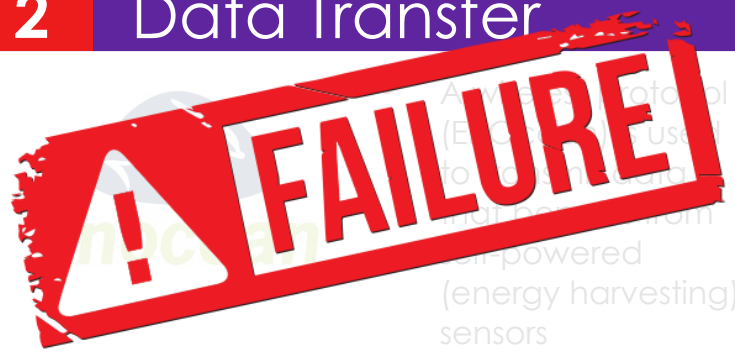


Ongoing validation of our proposals through discovery conversations with customers, suppliers & sector experts

How we tried to solve it

1 Sensors

2 Data Transfer



3 Gateway

4 Analytics

5 Visual Dashboard

6 Triggers

Fail Fast
Fail Cheap
Fail Early
Fail Often

Data Acquisition; We missed the obvious point! Opportunities come in three flavours:

Untapped Data

- In the environment today
- Not integrated
- Example – data on your PLCs or in the control environment

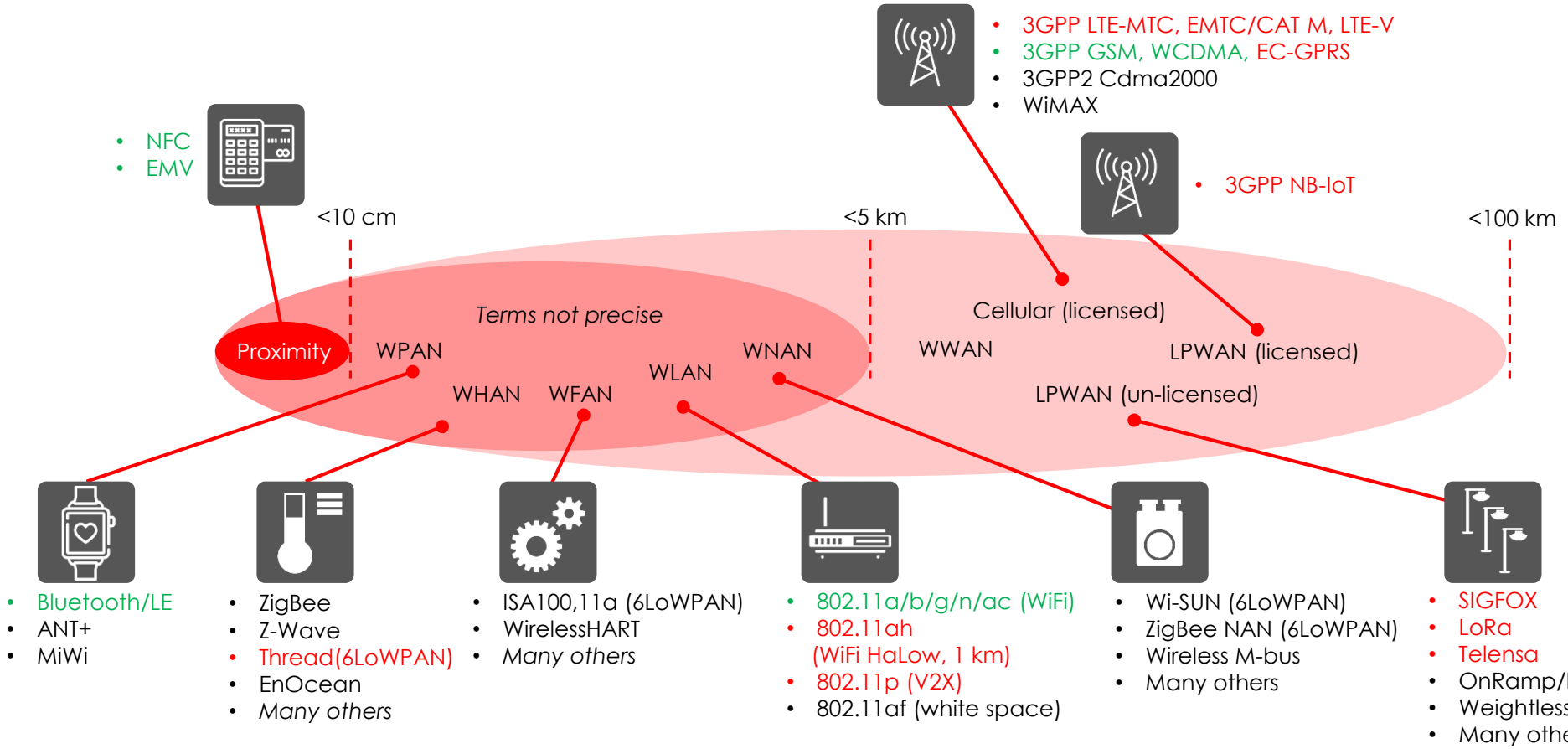
Stranded Data

- In the environment today
- Third-party integrated
- Example – data locked in the machine by the OEM

New Data

- New sensors and actuators

Communication: Wireless strengths and weaknesses



■ : > Billion units/year now

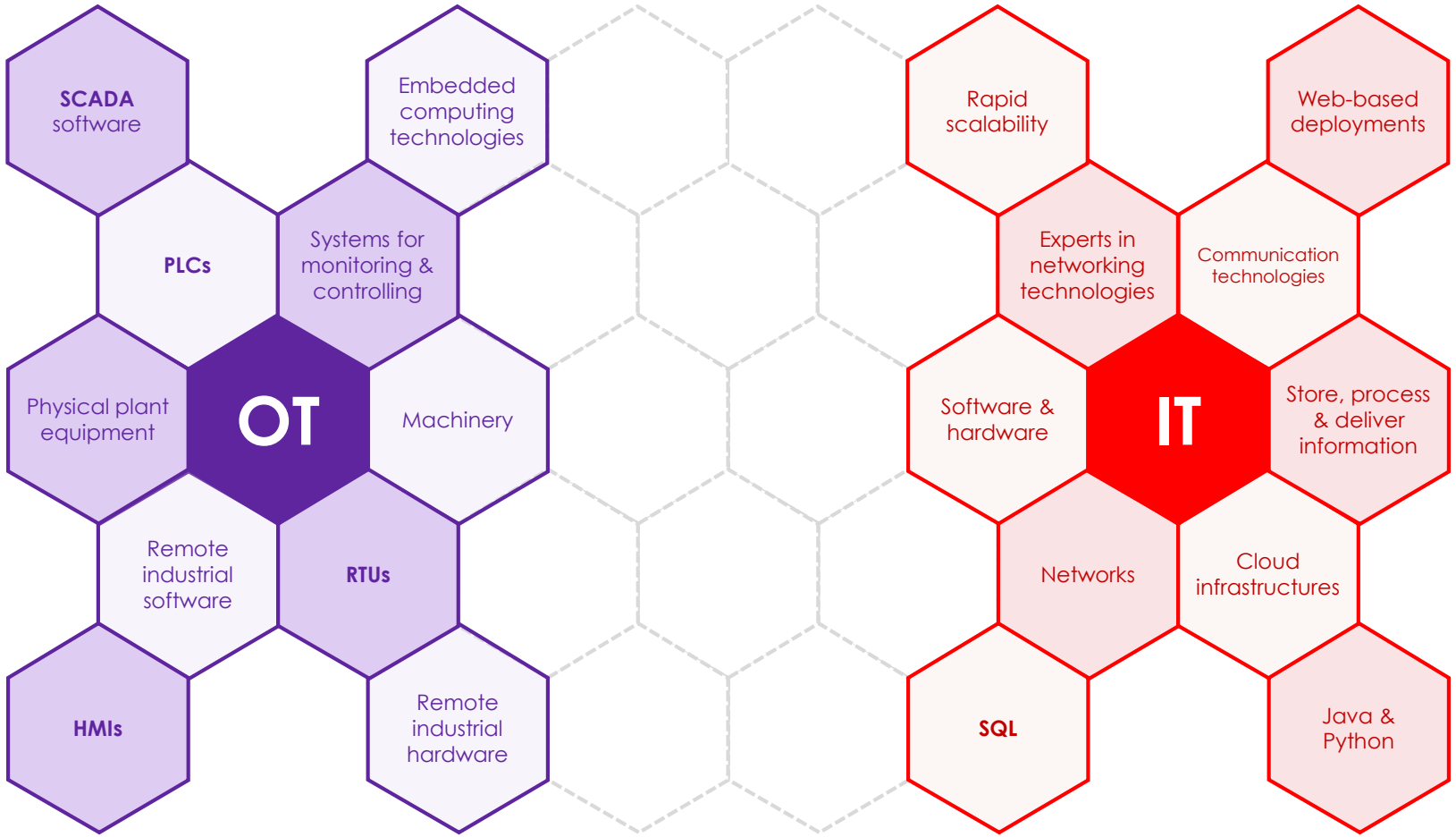
■ : Emerging

WPAN: Wireless Personal Area Network
WHAN: Wireless Home Area Network
WFAN: Wireless Field (or Factory) Area Network
WLAN: Wireless Local Area Network

WNAN: Wireless Neighbourhood Area Network
WWAN: Wireless Wide Area Network
LPWAN: Low Power Wide Area Network

LESSONS LEARNED

OT / IT integration capability is key

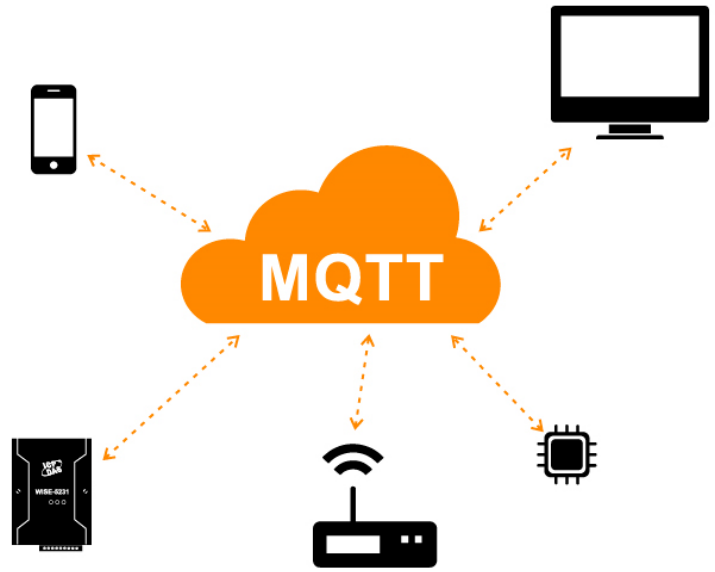


LESSONS LEARNED

OT / IT protocols need translation

OPC UA
Modbus
DeviceNet
EtherCAT
AS-Interface
EtherNet/IP
PROFIBUS
PROFINET
HART COMMUNICATION PROTOCOL
CAN
CANopen
CAN FD

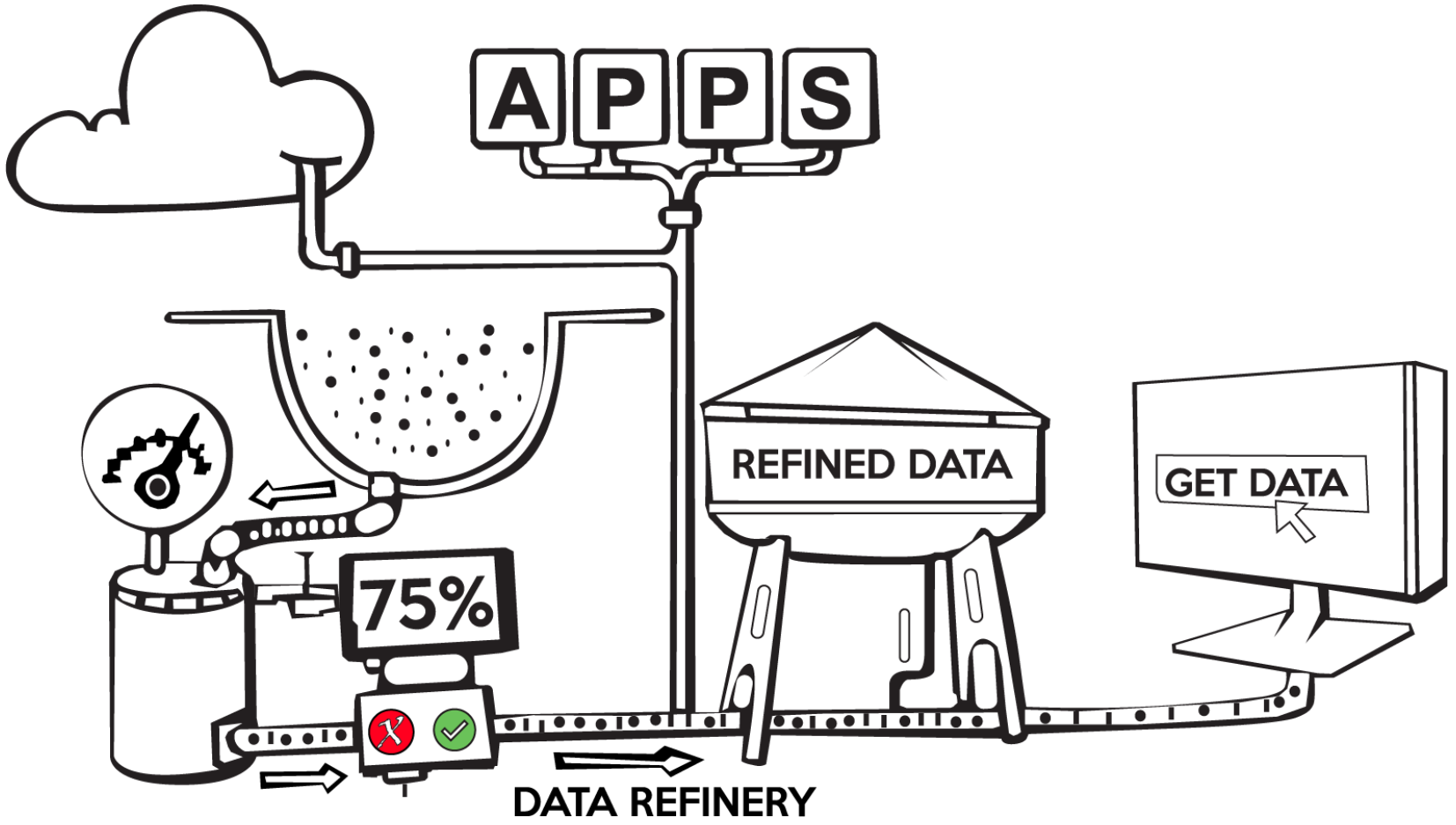
OT Protocols



Cloud Protocol

LESSONS LEARNED

You need reliable data to do data science!

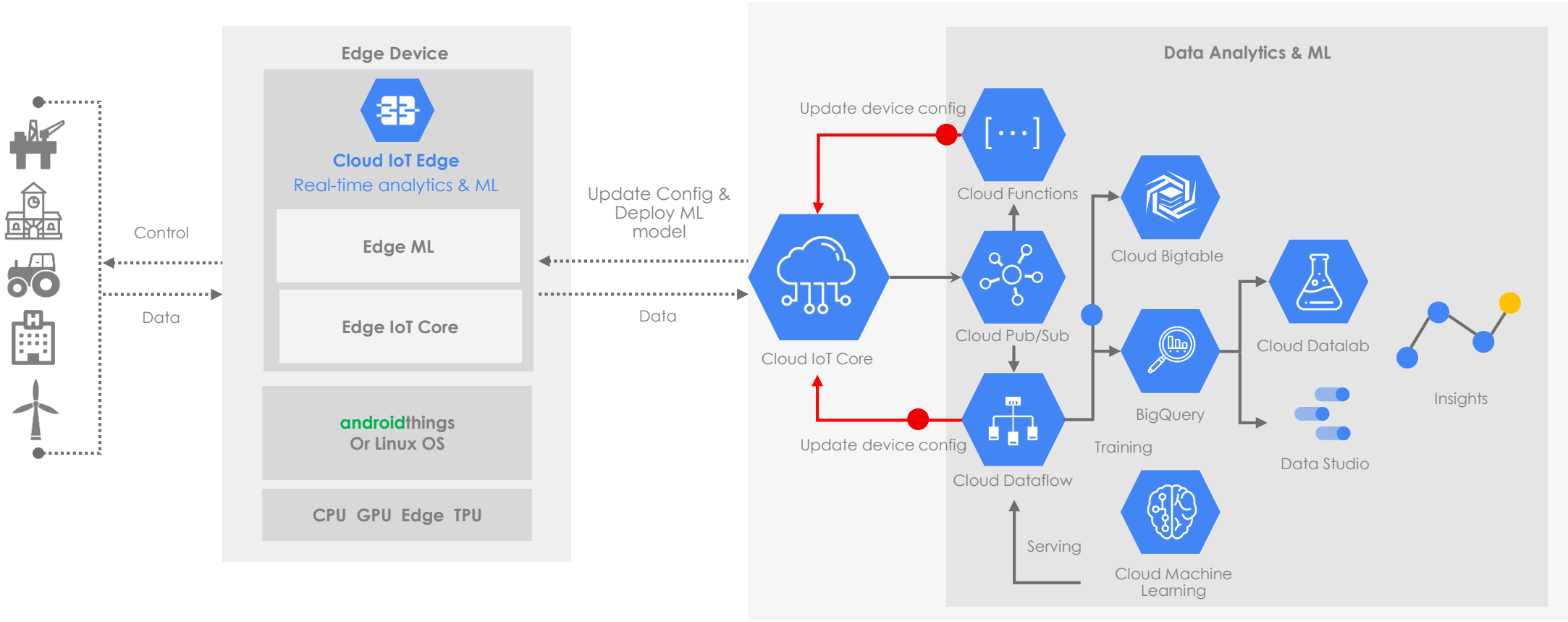


enocean

VOLUME

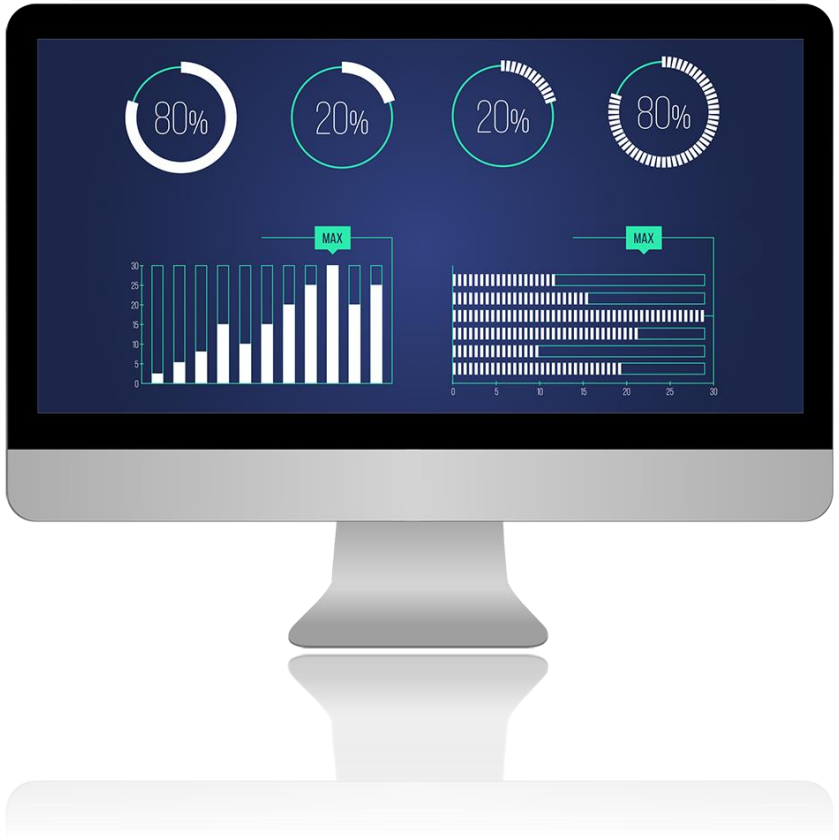
LESSONS LEARNED

Cloud architecture isn't easy to understand…
…it's even worse when it's not even in the cloud!



LESSONS LEARNED

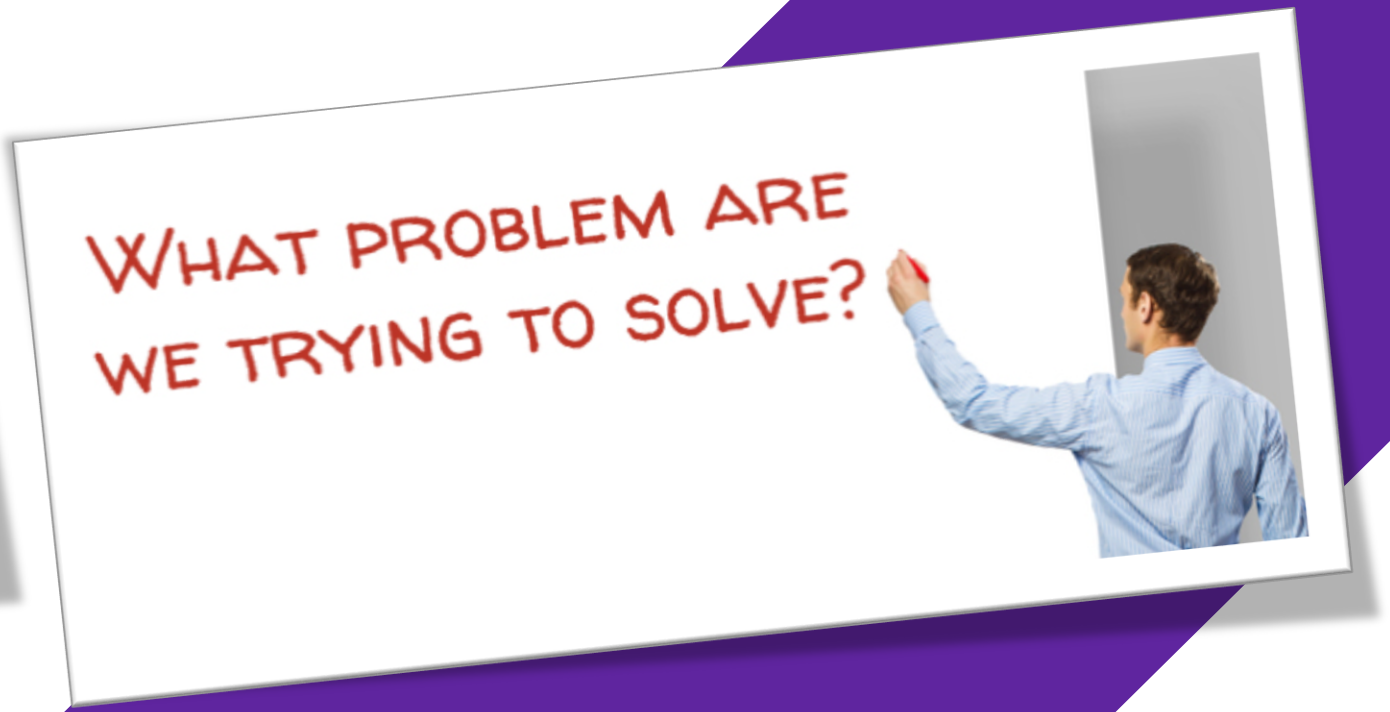
Everyone thinks they want a dashboard…
…but they don't, they want "calls to action"



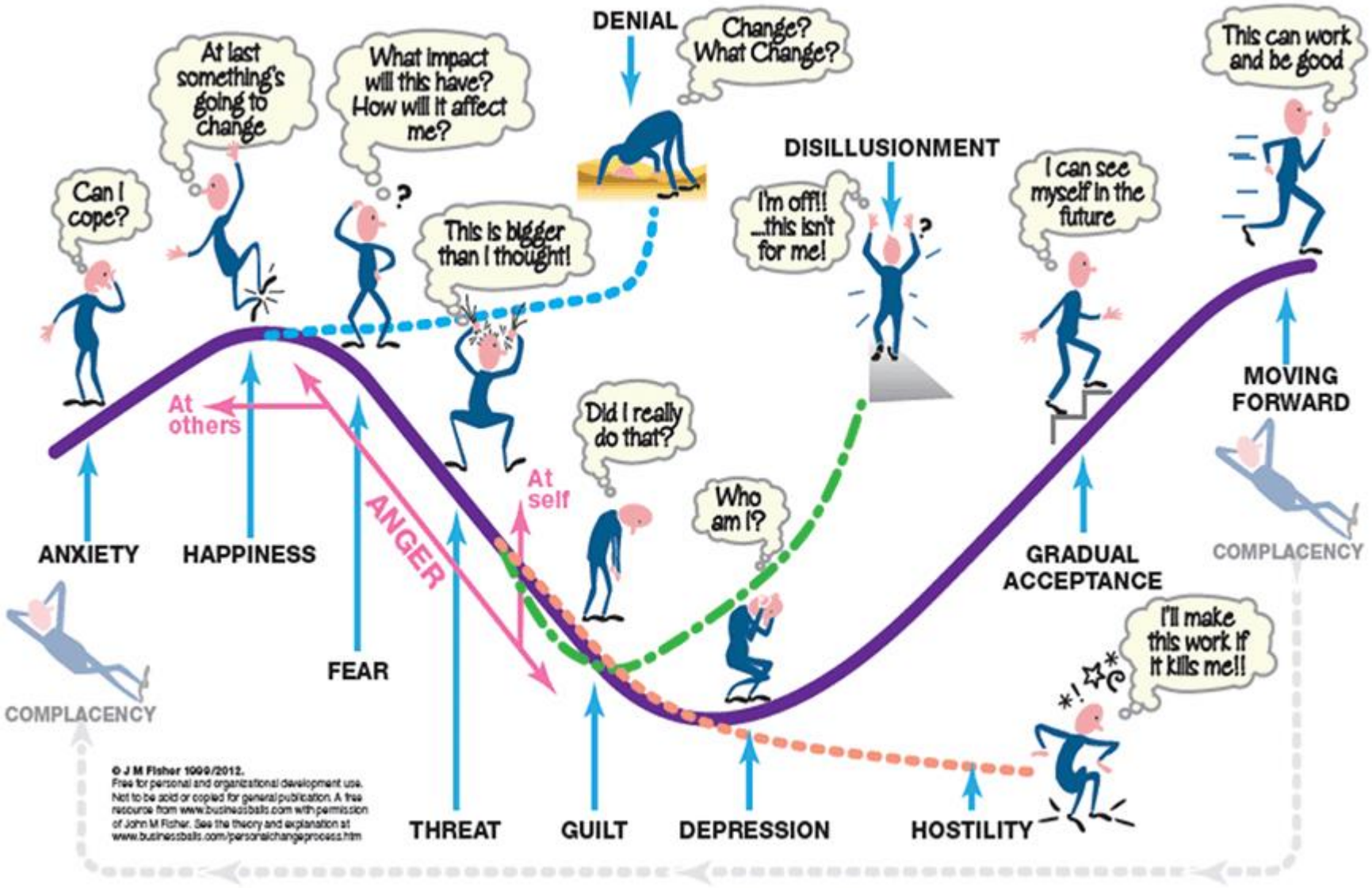
VS

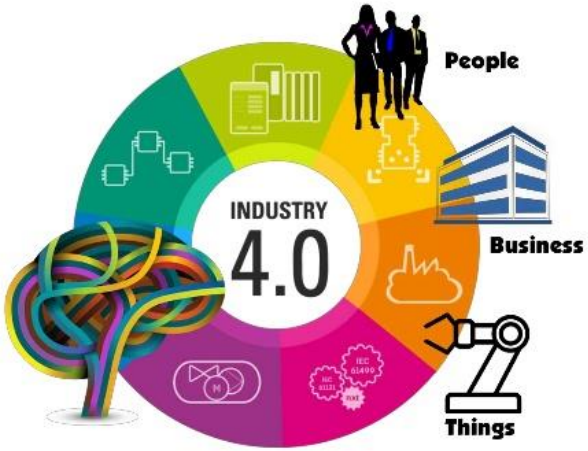
LESSONS LEARNED

What are we trying to do?



It’s all about people!





tips for starting with IIoT

Don't get hung up on the technology – be clear on the problem you're trying to solve

Put cyber security at the heart of the solution: ensure OT and IT are aligned to find a solution

Accept the fact you are an early adopter and the technology is not yet mature

Focus on aggregating the data that already exists before paying for new data

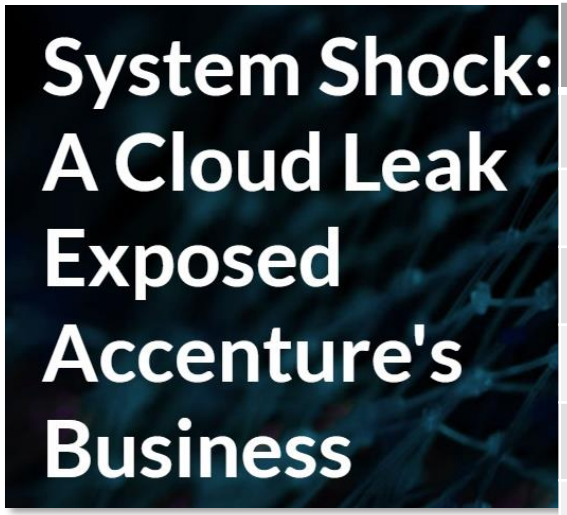
There's lots of possible partners out there: find one you are comfortable going on a journey with

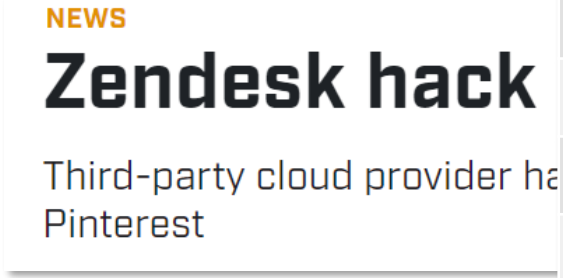
Work with experts – but become a well informed amature

05 Don’t Forget

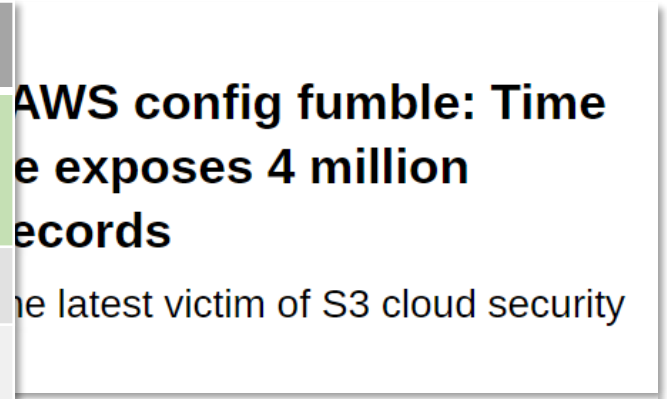
Hacking the factory

Software is complicated. People make mistakes.





No.	Vulnerability Description	Access	Affected Components	Reference
1	All the detail information has been reserved due to security concerns.	Local (USB)	HU_NBT	CVE-2018-9322
2		Local (USB/OBD)	HU_NBT	
3		Remote	HU_NBT	Logic Issue
4		Remote	HU_NBT	Reserved
5		Local (USB)	HU_NBT	CVE-2018-9320
6		Local (USB)	HU_NBT	CVE-2018-9312
7		Remote (Bluetooth)	HU_NBT	CVE-2018-9313
8		Physical	HU_NBT	CVE-2018-9314
9		Physical	TCB	Reserved
10		Remote	TCB	Logic Issue
11		Remote	TCB	CVE-2018-9311
12		Remote	TCB	CVE-2018-9318
13		Indirect Physical	BDC/ZGW	Logic Issue
14		Indirect Physical	BDC/ZGW	Logic Issue



Key takeaways

What to do

Passwords

Change default passwords and use strong passwords and multi-factor authentication wherever possible.

Do not use products with hard-coded passwords.

Stay Up-To-Date

Keep firmware and software updated (via automatic updates or monthly checks). Do not use products that cannot be updated. Closely follow the lifecycle of devices and remove them from service when they are no longer updatable.

Encryption

Enable encryption whenever possible so that data is never transmitted “in the clear.” Consider buying only devices that support encryption. Otherwise, consider using a VPN or other means to limit data exposure. .

Port Blocking

Ideally, block all incoming traffic but if this is not feasible, check for open software ports that may allow remote control and configure or restrict them as appropriate.

Separate Networks

Just as in guest networks, place IoT devices on a separate, firewalled and monitored network. This allows you to restrict incoming traffic, prevent crossover to your core network and analyse traffic to identify anomalies.

Disable unnecessary functions

Turn off any functionality that’s not needed, including cameras, microphones or even connectivity itself (e.g., if a smart TV is merely for display, not connectivity). It may also include physical blocking/covering of ports, cameras and microphones.

Limit Physical Access

Verify that physical access does not allow intrusion (e.g., by factory reset, easily accessible hardware ports or default password).

Limit Connectivity

Don’t allow (or severely restrict) connections via WiFi, Bluetooth or other means. This could even go as far as physically disabling features e.g. removing aerials and network device isolation if a device only needs to talk to the local router.


Questions?

Read Our Full Report Online

Search ‘Going Fourth’ or ‘Industry 4.0’ on irwinmitchell.com

Visit https://irwinmitchell.turtl.co/story/going-fourth-data-industry-40-and-the-future-of-manufacturing/

irwinmitchell

Key Contacts

Dorrien Peters

Partner and National Head of Manufacturing

+44 (0)114 274 4947
+44 (0)7710 381 523
dorrien.peters@irwinmitchell.com

Melanie Bancroft

Business Development Manager

+44 (0)114 274 4489
+44 (0)7918 738 251
melanie.bancroft@irwinmitchell.com

Kirsty Ayre

Partner and Head of Sheffield Employment Team

+44 (0)114 274 4911
+44 (0)740 773 3385
kirsty.ayre@irwinmitchell.com

Expert Hand. **Human Touch.**

To Get involved with Northern Crucible

Contact Sean Ibrahim

O7967 009749

irwinmitchell