Indegy

Industrial Cyber Security

Unveiling Security Gaps in ICS Networks

- Confidential -

Today's Webinar

Unveiling Security Gaps in ICS Networks

Presented By:
Mille Gandelsman, CTO, Indegy

©2016 Indegy

Top Concerns as an ICS manager

What’s missing in ICS environments?

Security gaps in an ICS network

1. *Understanding what you have in your network*
2. *No visibility into critical control-layer activity*
3. *Blindspots of physical access to devices*

What’s missing in ICS environments?

Top Concerns as ICS manager

- How do I ensure my revenue generating process keeps running?
- How quickly will I discover a failure?
- How quickly can I pinpoint the source of the incident?
- How quickly can I recover?

©2016 Indegy

Top Concerns as an ICS manager

What’s missing in ICS environments?

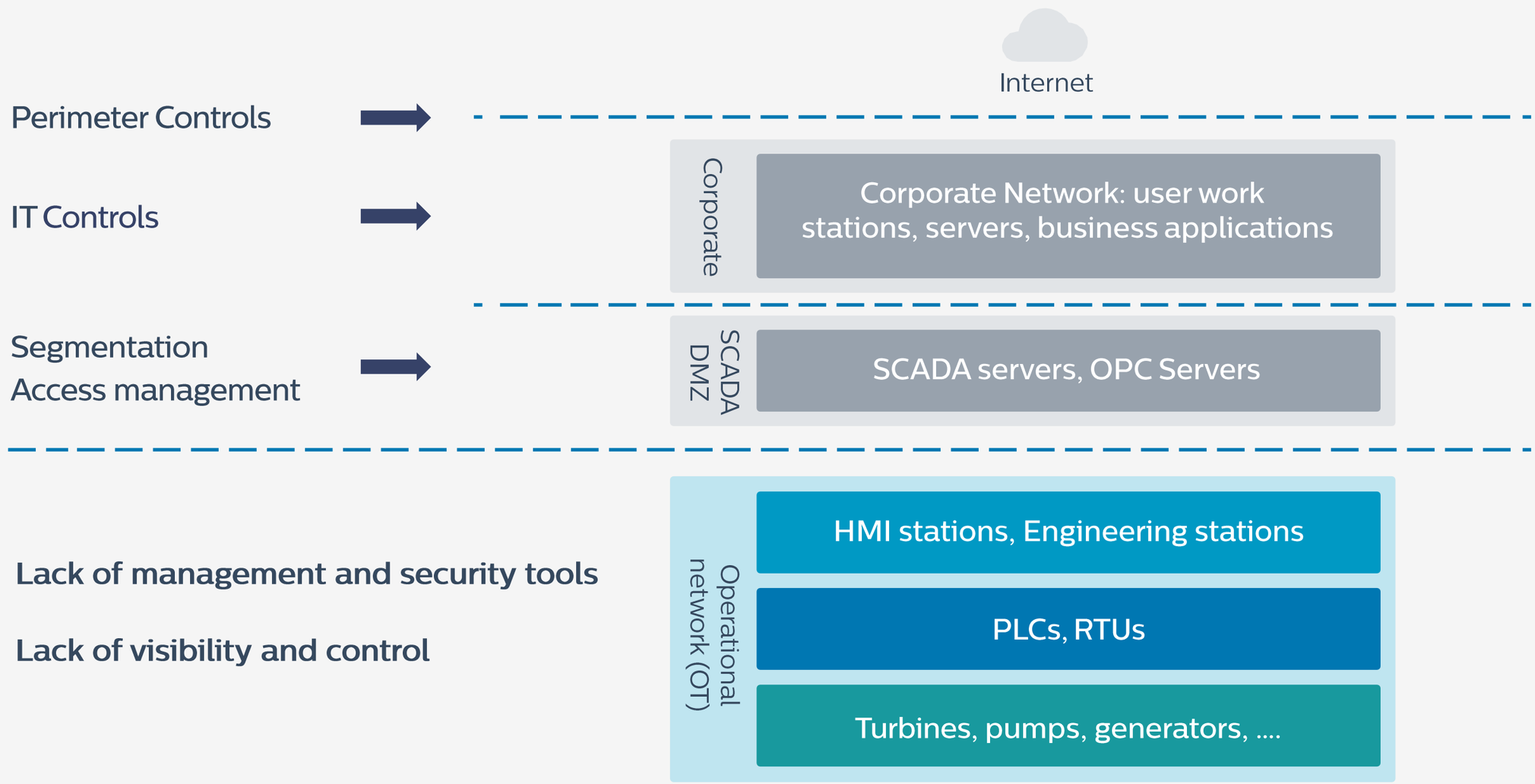
Security gaps in an ICS network

1. *Understanding what you have in your network*
2. *No visibility into critical control-layer activity*
3. *Blindspots of physical access to devices*

What’s missing in ICS environments?

- Confidential -

Visibility in the Operational Network

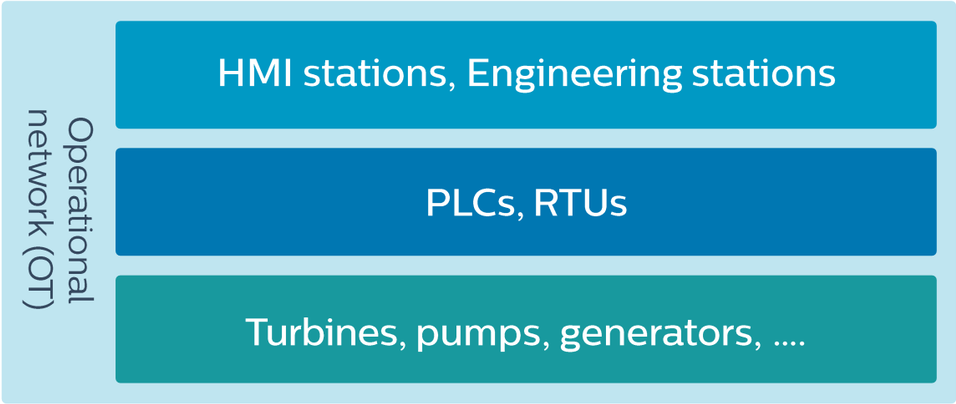


- Lack of management and security tools
- Lack of visibility and control

©2016 Indegy

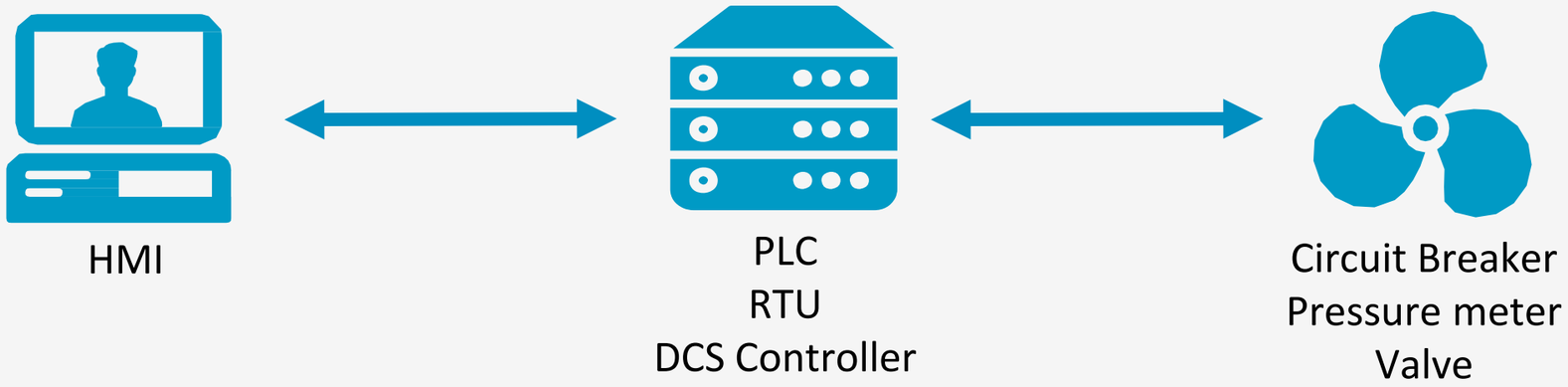
- Confidential -

Vocabulary & Definitions



SCADA / DCS –Supervisory, Control And Data Acquisition system (or a distributed one):

- HMI, Engineering station – Windows machines for operators to interact with system
- PLC/RTU/Controller – Dedicated 24/7 real time Industrial computers
- Sensors/Actuators/IO – Industrial Equipment (Turbines, Pumps, Valves, etc.)



©2016 Indegy

Top Concerns as an ICS manager

What's missing in ICS environments?

Security gaps in an ICS network

1. Understanding what you have in your network

2. No visibility into critical control-layer activity

3. Blindspots of physical access to devices

What's missing in ICS environments?

- Confidential -

The Security Gaps in ICS networks

Security Gap #1

Understanding what you have in your network

©2016 Indegy

- Confidential -

Asset Discovery and Management

- System implemented a very long time ago
  - Changes made over years
  - Without documentation

- Or it was recently inherited
  - Nobody knows anything

Discover the assets in your network

©2016 Indegy

What do I know about my assets?

- The details I need:
  - IP / MAC / Serial address
  - OS / Firmware versions
  - When were they last updated? By who?
  - Associated risk of the device
  - List of potential vulnerabilities

- The details are constantly changing over time
  - Usually through a manual process
  - Error prone
  - Documentation-less

Monitor the changes in your assets

©2016 Indegy

- Confidential -

The Security Gaps in ICS networks

Security Gap #2

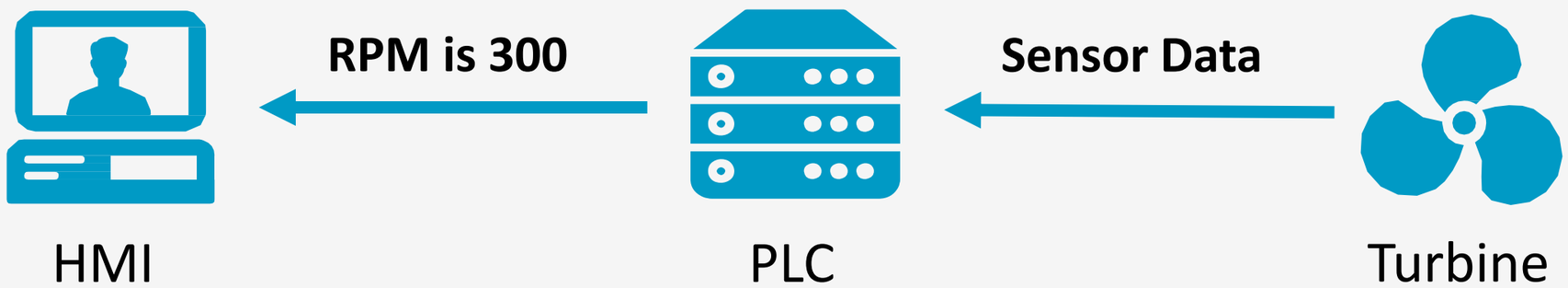
No visibility into critical control-layer activity

©2016 Indegy

- Confidential -

Day to day operations

- Operator reads data from the system



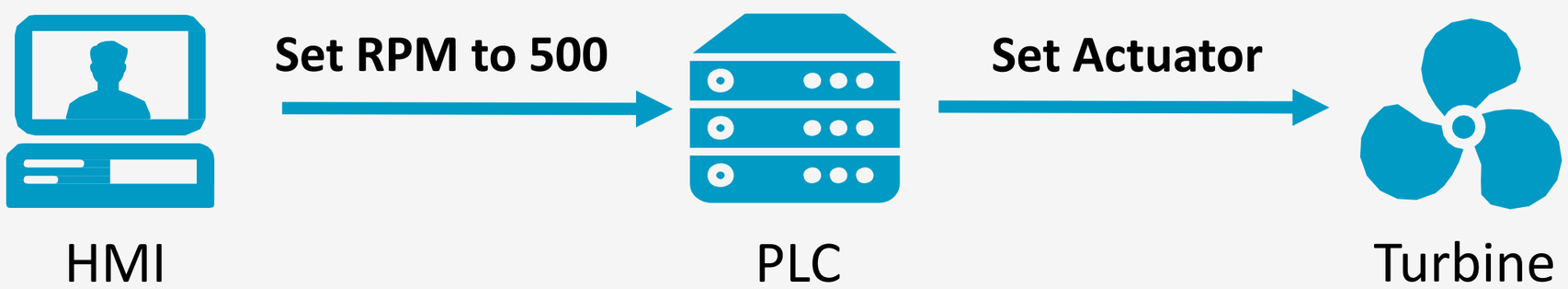
©2016 Indegy

- Confidential -

Day to day operations

- Operator reads data from the system

- Operator changes process parameter

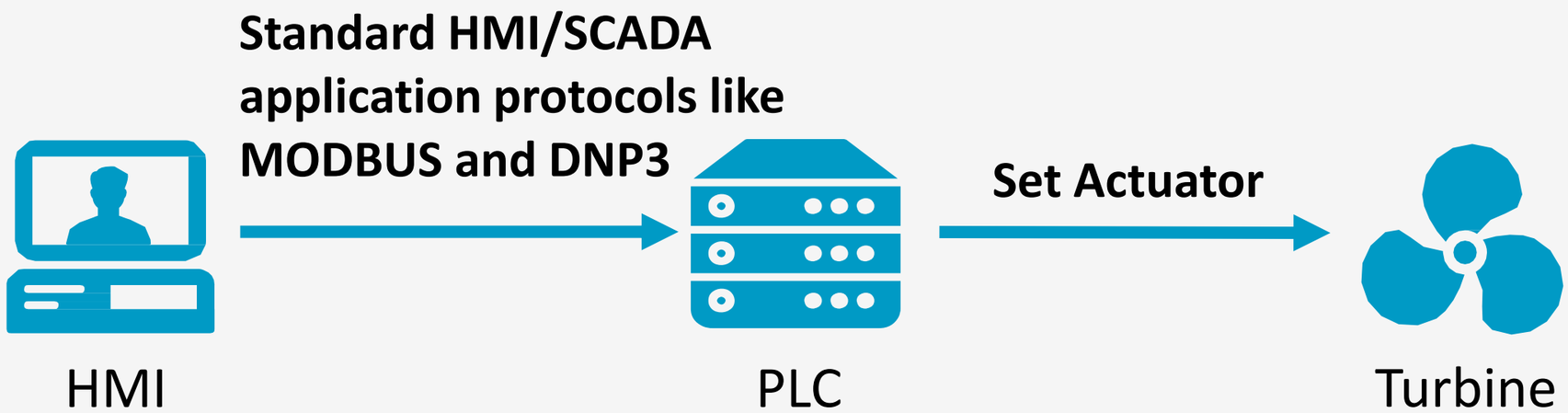


©2016 Indegy

- Confidential -

Monitoring ICS Network Activity

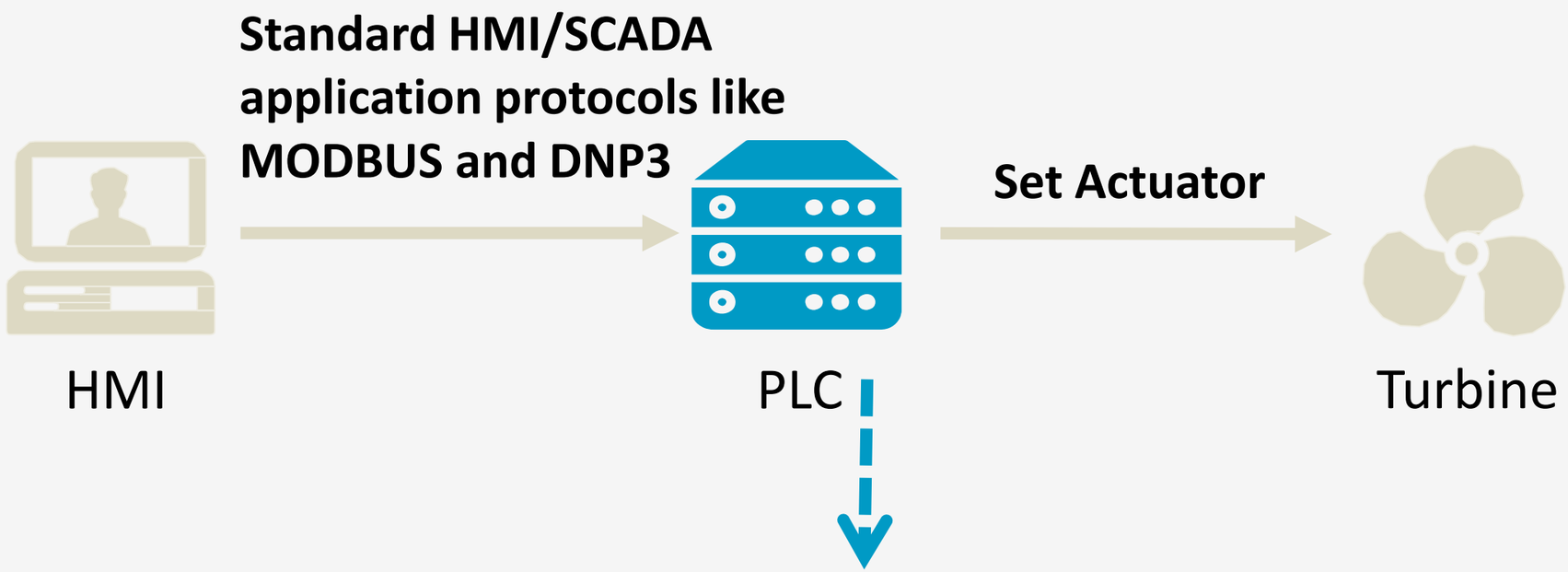
Nothing like monitoring IT Networks



©2016 Indegy

Monitoring ICS Network Activity

Nothing like monitoring IT Networks



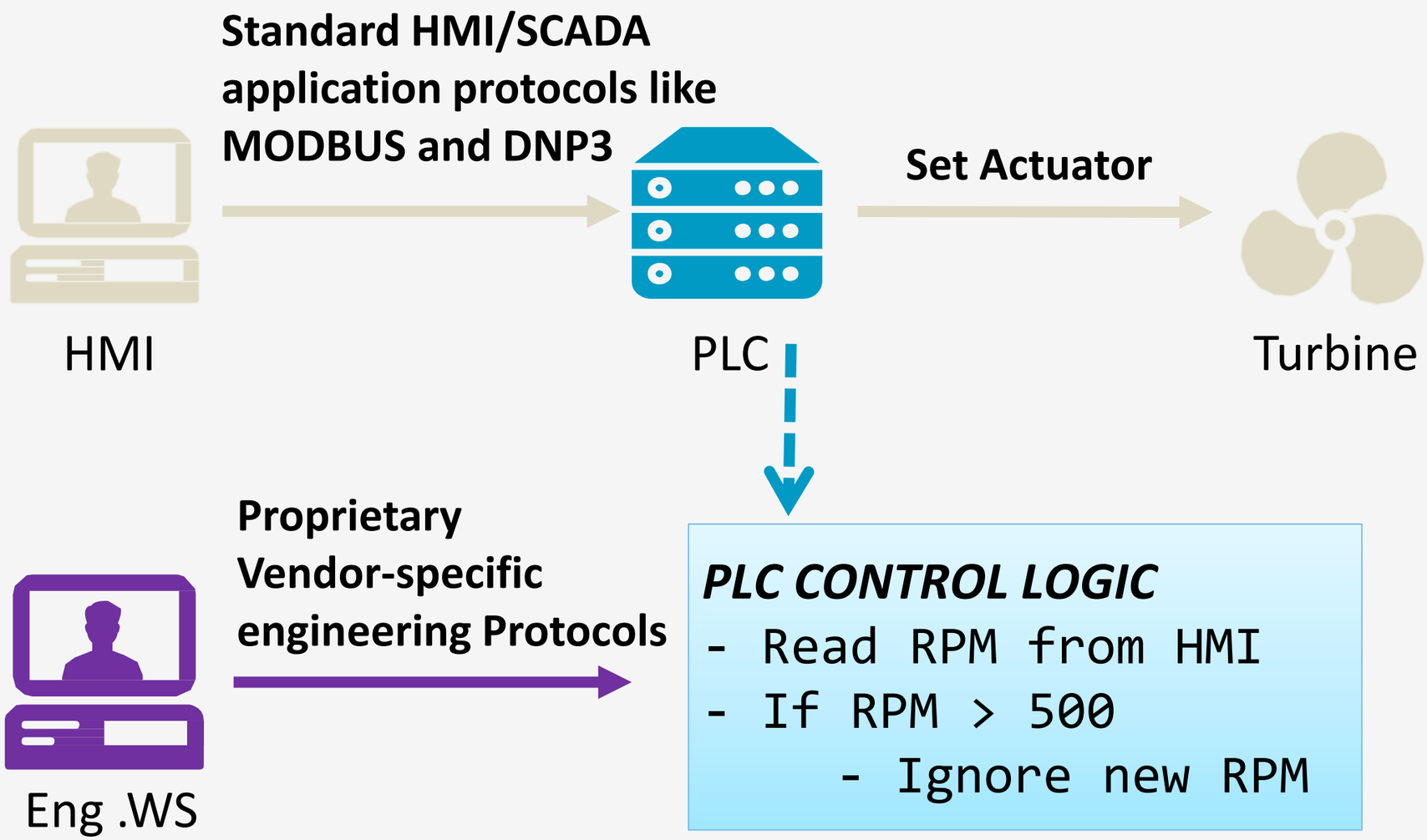
PLC CONTROL LOGIC

```
- Read RPM from HMI
- If RPM > 500
      - Ignore new RPM
```

©2016 Indegy

Monitoring ICS Network Activity

Nothing like monitoring IT Networks



©2016 Indegy

- Confidential -

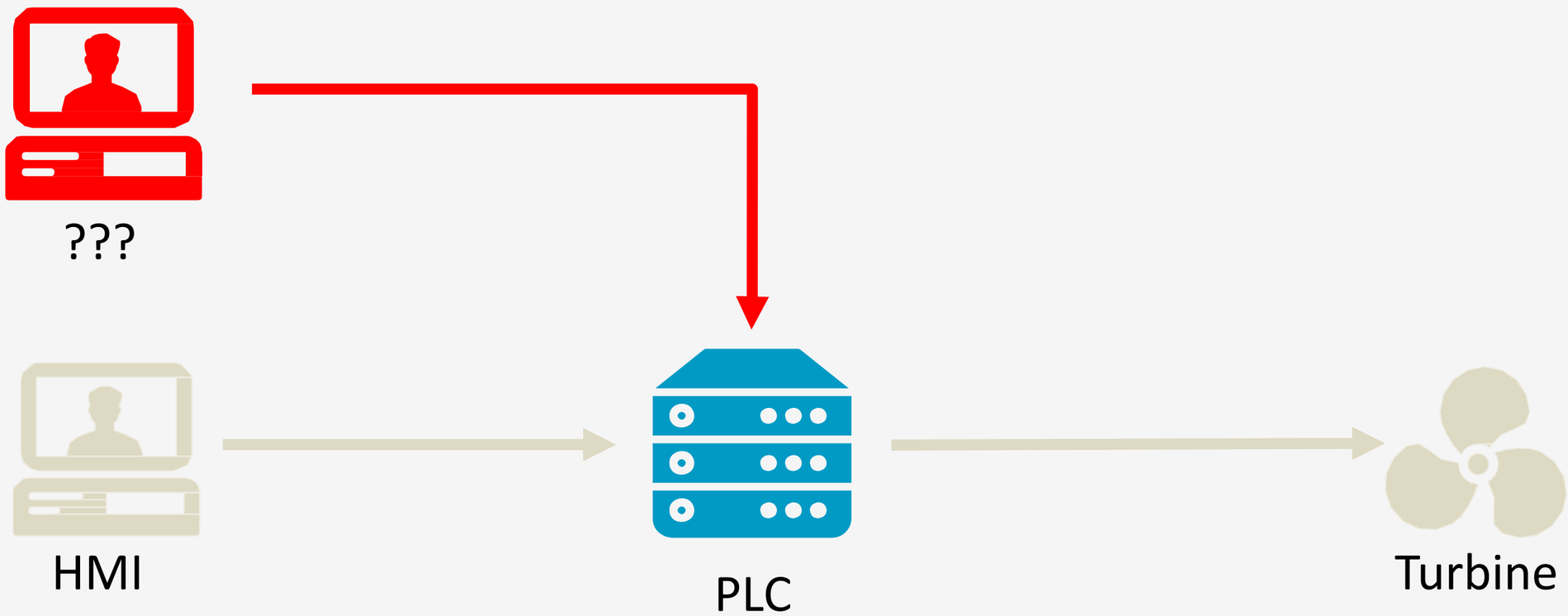
A couple of problems

- No Authentication Required:
  - Anyone with network access can change controller logic!
- Difficult to monitor:
  - Hard to identify changes to controller logic

(Note that there is no need to exploit vulnerabilities…)

©2016 Indegy

Anatomy of an ICS Attack

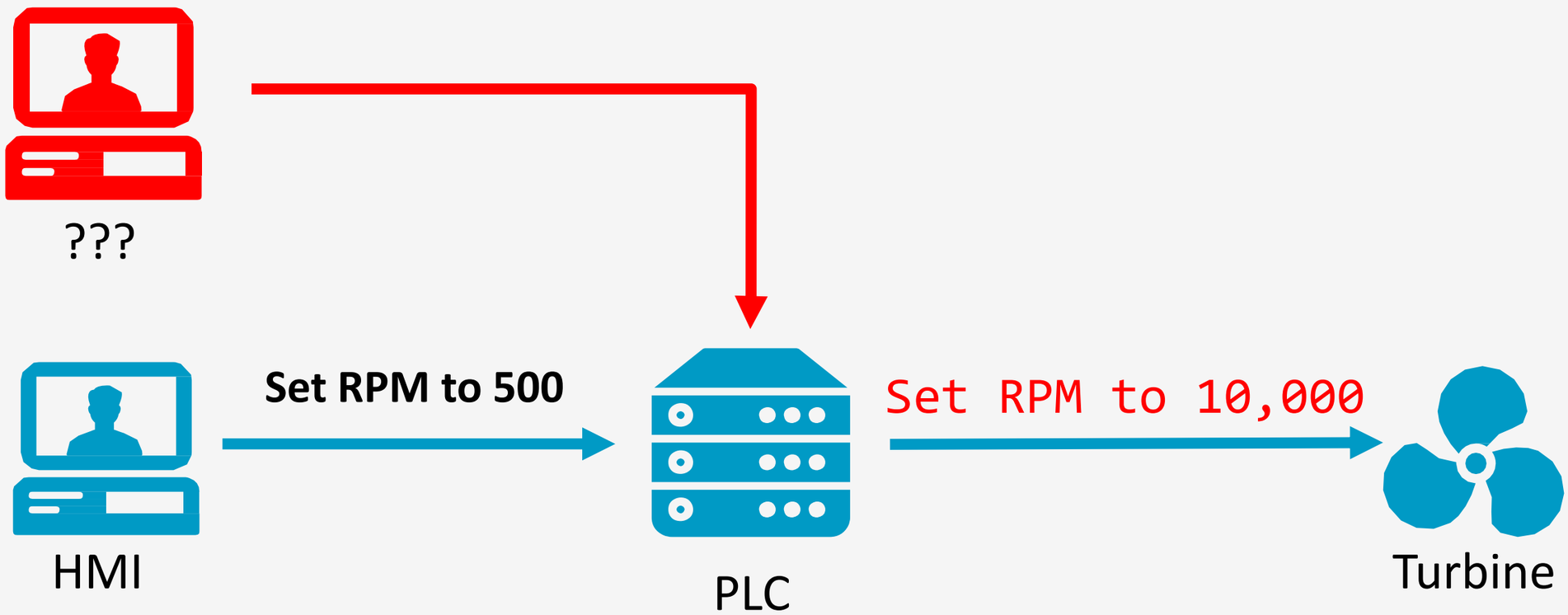


PLC CONTROL LOGIC

```
- Read RPM from HMI
- Always set RPM to 10,000
```

©2016 Indegy

Anatomy of an ICS Attack



PLC CONTROL LOGIC

```
- Read RPM from HMI
- Always set RPM to 10,000
```

©2016 Indegy

- Confidential -

ICS Network Visibility and Control

Monitoring control-layer activity is essential!

©2016 Indegy

- Confidential -

The Security Gaps in ICS networks

Security Gap #3

Blindspots of physical access to devices

©2016 Indegy

- Confidential -

Changes Made Directly on Physical Devices

- On-The-Fly-Changes
  - What changed?
  - What was the previous config?
- System integrator access
  - Who to blame on failure?

©2016 Indegy

Top Concerns as an ICS manager

What’s missing in ICS environments?

Security gaps in an ICS network

1. ***Understanding what you have in your network***
2. ***No visibility into critical control-layer activity***
3. ***Blindspots of physical access to devices***

What’s missing in ICS environments?

- Confidential -

What's missing in ICS environments?

Visibility!

To assets and to control-layer changes

Run the "Would I know about a change" test

©2016 Indegy

Indegy

Securing Against **Operational Disruptions** caused by **Cyber Threats, Malicious Insiders and Human Error**, by providing **Visibility and Control** to industrial networks.

Taking the first steps towards ICS security

Do you know what needs to be protected?

1

Know what needs to be protected

2

Monitor on-going activities

3

Apply policies, Get real-time alerts

Reliable and extensive ICS device inventory

©2016 Indegy

Taking the first steps towards ICS security

What is happening within the OT Network?

1

Know what needs to be protected

2

Monitor on-going activities

3

Apply policies, Get real-time alerts

Dangerous changes are in the **control-layer** communications

©2016 Indegy

Taking the first steps towards ICS security

Can you effectively manage and respond to events?

1

Know what needs to be protected

2

Monitor on-going activities

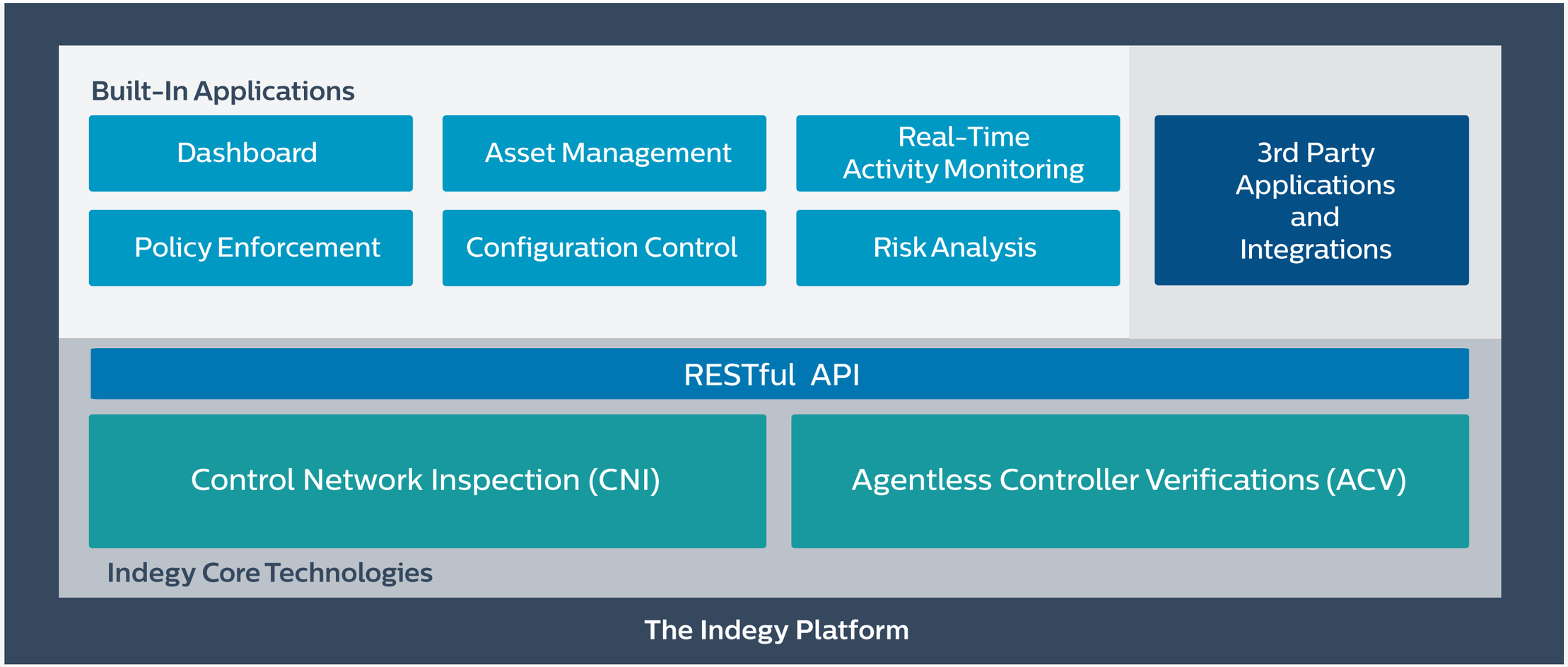
3

Apply policies, Get real-time alerts

Without **visibility** you can't have security

©2016 Indegy

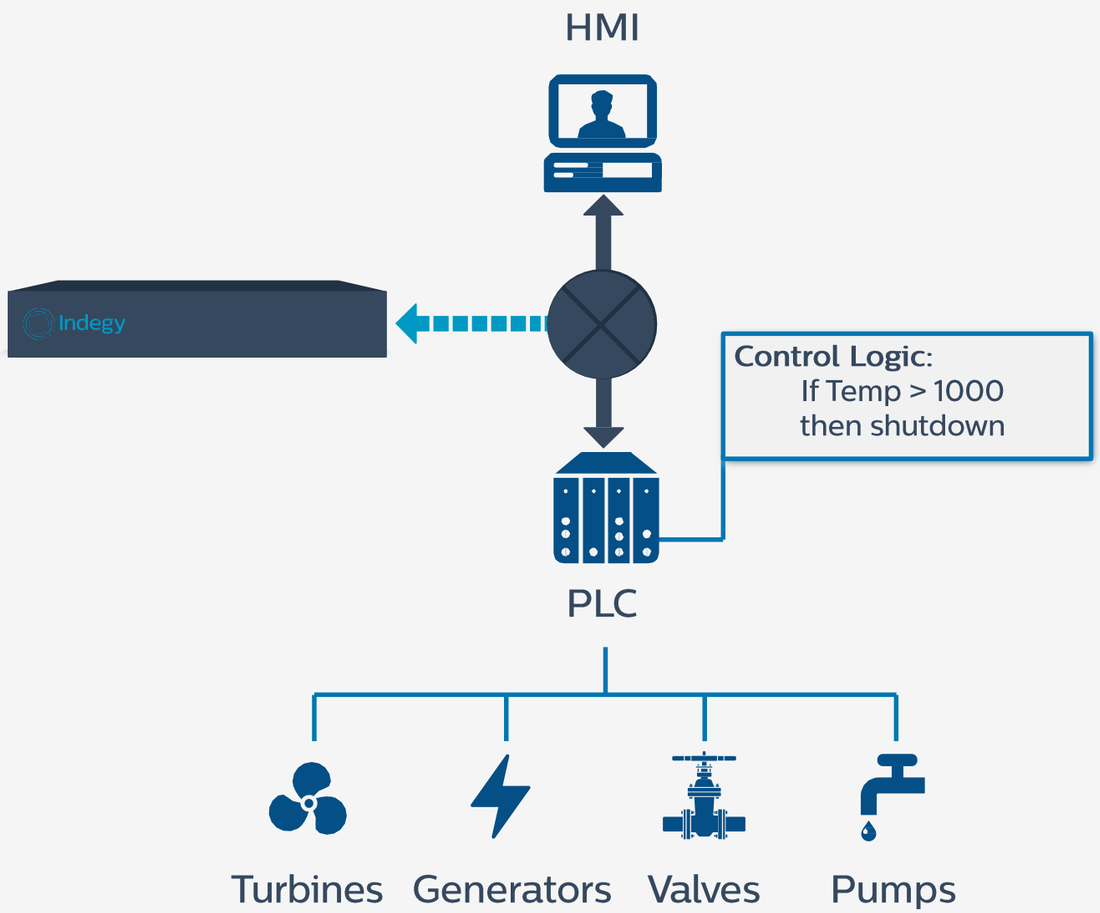
The Indegy Platform



©2016 Indegy

- Confidential -

Control Network Inspection (CNI)

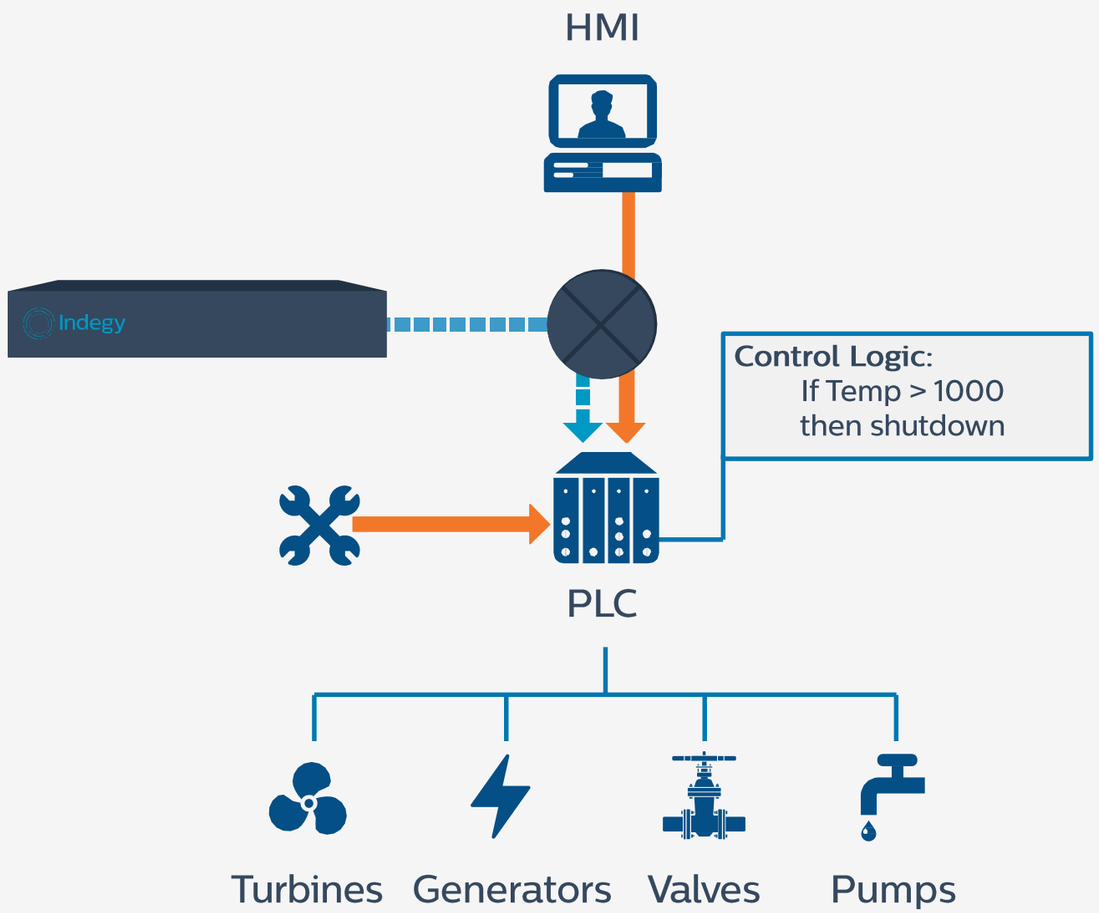


- Passive network activity monitoring
- Deployed on mirror port or network tap
- Deep understanding of ICS protocols
- Including vendor-specific IEC-61131 standard PLCs implementations
- Real-time visibility into all OT activity

©2016 Indegy

- Confidential -

Agentless Controller Verification (ACV)



- Patent-pending technology
- Periodic verification of controller state
- Validates configuration, code and firmware
- Captures all changes – network and direct
- Eliminates operational blind spots

©2016 Indegy

- Confidential -

Security and Operations – Hand in Hand

Industrial Cyber Security

- Real Time Activity Monitoring
- Risk Analysis
- Support Forensic Investigations

+

Operational Value

- Asset Inventory
- Configuration Management
- Change Management

©2016 Indegy

Indegy

Industrial Cyber Security

Thank you!

Want to know more?
Contact us: info@Indegy.com

Indegy provides situational awareness and real-time security for industrial control networks to ensure operational continuity and reliability.

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

PRESENTED BY

Michael A. Marullo

InfoNetrix LLC

New Orleans, Louisiana USA

JULY 29, 2016

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

About InfoNetrix…

- Independent Market Research & Consulting Firm launched January 2002
- Client Base of over 150 automation/IT suppliers, users, consultants & TPPs
- Conducted >25,000 Primary Research Interviews with automation/IT professionals
- Main Market Focus Areas:
  - ENERGY: Conventional & Alternative Sources
  - UTILITIES: Electric, Gas & Water
  - COMMUNICATIONS: Public & Private Networks & Equipment
- Other Target Markets:
  - TRANSPORTATION: Land/Air/Sea
  - GOVERNMENT: Including Military
  - FACILITIES: Buildings & Spaces
- Major Accomplishments:
  - VISTA Smart Grid Horizons™ Study: *"Automation in the North American Grid Transformation Marketplace; 2009-2014"*
  - *LegacyPro™ Database*: >35,000 records of North American electric utility automation/IT projects

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

Today's Presentation…

- **Purpose:** To put forward a new way of thinking about Infrastructure that embraces the employment of intelligence – automation, monitoring, control, etc. – at the earliest stages of infrastructure Planning, Design & Development, rather than as an afterthought, as has often been the case thus far.
- **Scope:** The need for Intelligent Infrastructure spans multiple industries and markets. Today we will explore some recent examples of infrastructure that is *'Intelligent by Design'* and how that approach can help to overcome the major challenges we face in the form of Aging Workforce and Declining Infrastructure, which collectively threaten both current and future infrastructure reliability and sustainability.

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

Question: **What is meant by the term…**
Intelligent Infrastructure?

Answer: ***Infrastructure that is inherently planned, designed and developed with intelligence that is built in… NOT bolted on.***

A different way of thinking about infrastructure…

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

Background

- For the past 50 years, infrastructure has been routinely planned, designed, built and deployed 'serially' with little or no thought given to how it would be monitored/controlled after deployment.
- Even in cases where a separate RFP has been issued for automation of the infrastructure, that 'intelligence' has most often been installed during or after construction/deployment – in other words 'bolted on' after the fact.
- Although big, expensive, environmentally fragile solutions of the times perhaps offered some valid reasons that is no longer the case – but we continue to act as if those limitations remain.

Later in this presentation we'll take a look at some examples, but for now, let's get back to what we mean by *Intelligent Infrastructure*…

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

Isn't Intelligent Infrastructure the same as IoT and IIoT?

The simple answer is no… and here's why:

- IoT (*Internet of Things*): While *Intelligent Infrastructure* embraces *IoT* and the Internet certainly plays an important role, it isn't the same. Building intelligence into infrastructure is a fundamental concept involving a different approach to the planning, design and development of infrastructure. *IoT* is simply an example of an *enabler* of that concept.
- IIoT (*Industrial Internet of Things*): This is getting closer, but there are still both practical and philosophical differences, especially since *Intelligent Infrastructure* is not exclusively a function of the Internet nor is it exclusively 'industrial' in nature.

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

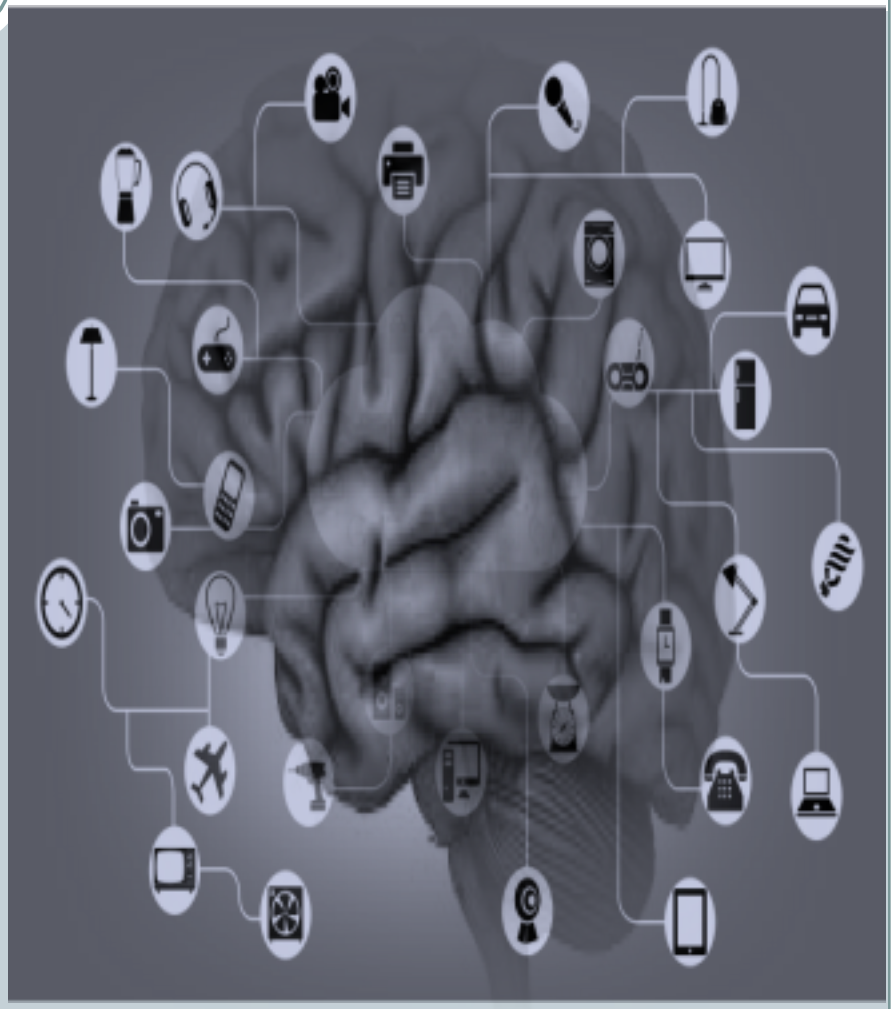
Intelligence That's Built In – Not Bolted On!

Then what IS *Intelligent Infrastructure?*

Making infrastructure intelligent is more than just hooking up a bunch computers up to new and/or existing infrastructure.

Although some of that will be necessary for infrastructure to become truly intelligent, it will take more – much more – to overcome the challenges ahead. Instead…

Intelligence needs to be in the "DNA" of our infrastructure… from planning and design through development, deployment and support.



© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

BIG CHALLENGES ~~COMING~~ NOW!

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

What if???

What would happen if 60,70 or even 80 percent of all vehicles on the road became inoperable over a period of a few years – and, the mechanics needed to fix them were either retired or had just moved on?

Sounds crazy, huh?

Not really. We're already at that point with critical infrastructure. Plus, the highly skilled, experienced people who designed, built and have been supporting that infrastructure for decades (the 'mechanics') are simultaneously reaching retirement age – a 'perfect storm' like we've never, ever seen before!

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

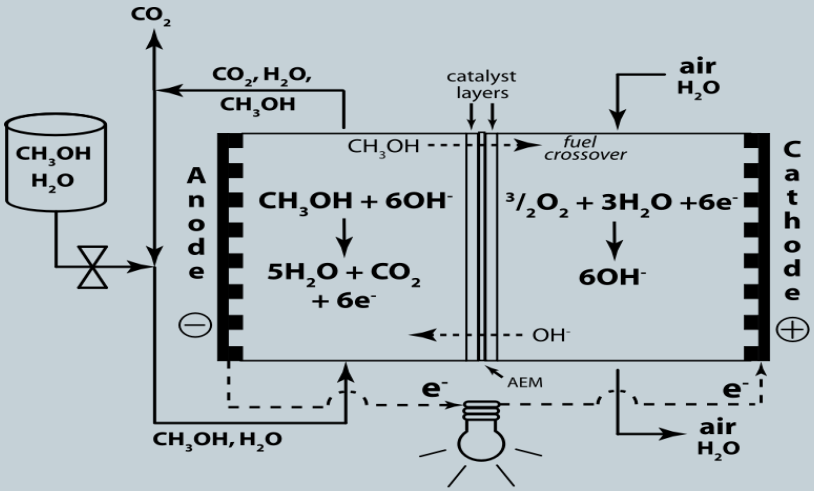
Intelligence That's Built In – Not Bolted On!

And then, there's this…

Let's assume that we could just "find the money" to replace that failing infrastructure… who we would get to do it?

Colleges and universities have not been graduating enough STEM (Science, Technology, Engineering & Math) students to fill even the entry-level jobs being vacated.

And, the more advanced positions – those requiring specialized technical knowledge, skills and experience – will be even harder to fill. (Yikes!)



© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

Aging Workforce Fact: About 10,000 Baby Boomers reach retirement age every day – a trend that will continue for the better part of the next two decades!

Declining Infrastructure Fact: Large portions of our existing infrastructure are near, or have already reached, the end of their statistically projected 35- to 50-year useful life expectancy.

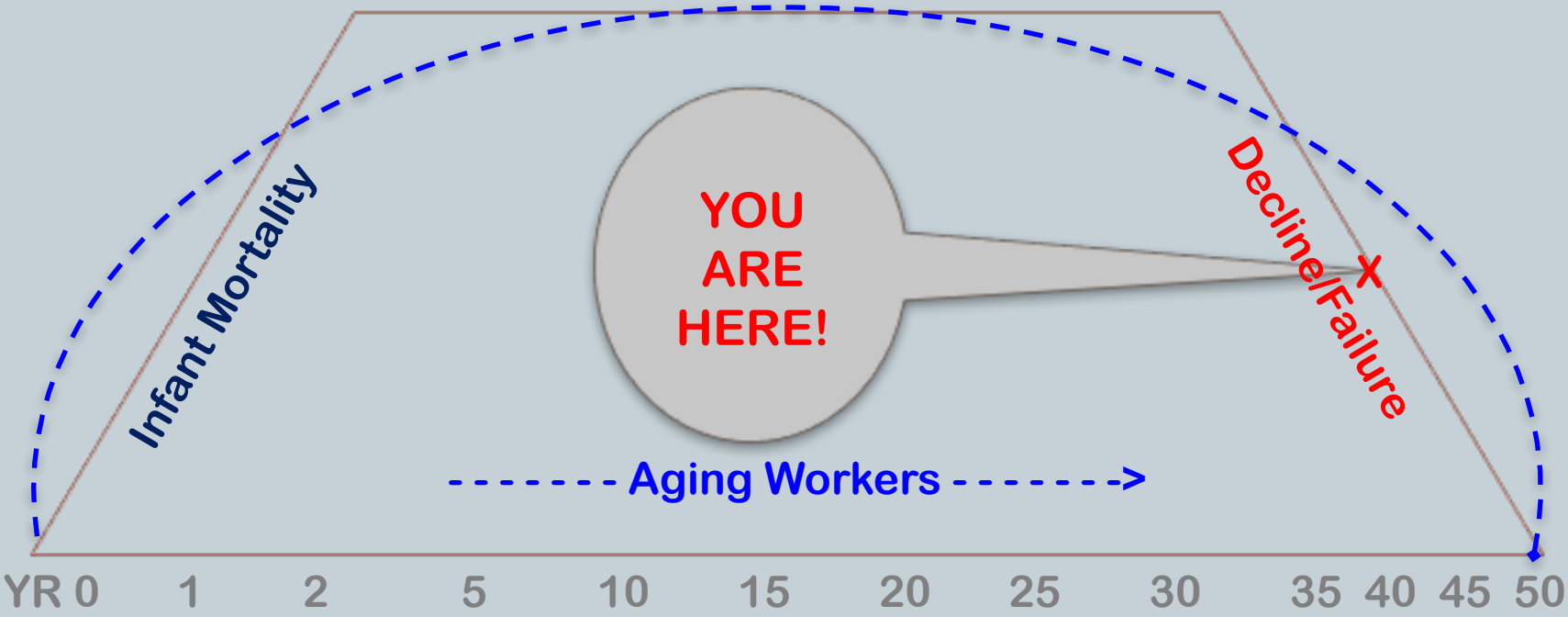
© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

EQUIPMENT RELIABILITY LIFE CYCLE*

← Extended Period of Sustained Reliability →



*Average is 35-50 Years from Infant Mortality to Decline & Failure

(NON-LINEAR SCALE USED FOR ILLUSTRATION PURPOSES ONLY)

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

LESSONS FROM THE INFORMATION AGE

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

Lessons from the Information Age…?

What we often refer to as the "Information Age" produced a lot more raw *data* than it did actionable *information*. It rightfully should have been called *The 'Data' Age!*

Most of the time, the goal wasn't as much about making the process better as much as it was about simply trying to understand it better by gathering more data – LOTS of it. Back then…

- Voluminous reports were systematically printed on 'green bar' paper or stored on a tape, a disk or some other medium and filed away –never to be seen again.
- Alarm logs, inventory lists, production records and myriad reports were meticulously stored away warehouses – more recently in 'data silos' – that few personnel even know how to find, should they be needed.

These are old habits that we learned a long time ago and continue today – but a lot of the time, no one really knows why. Lessons learned, right?

Let's put this into context…

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

The Way We Did the Things We Did

Let's say that in 1970 you had three crews of three people each, plus three supervisors and a fleet of five trucks equipped with the tools and equipment to perform routine and remedial field inspections 24/7/365.

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

The Way We Did the Things We Did…

Round 1: The first round of modernization involved putting the schedules and maybe even the trucks, tools and inventory, into a spreadsheet or database and giving shift supervisors access via a computer terminal that could display the information. (NOTE: At that time, no one wanted solutions that might narrow job opportunities or eliminate workers!)

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

The Way We Did the Things We Did…

- **Round 2:** Later on, although things got more sophisticated, hardly anyone was actively thinking about applications like comparing shift efficiencies, keeping track of hours worked to comply with OSHA rules or analyzing vehicle maintenance and performance records across fleets.

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

The Way We Did the Things We Did…

- **Round 3:** Some of the reasons automation was so underutilized 'back then' was the fear of job losses, plus the fact that some of the requisite technology was not yet available – or in some cases, not yet affordable.
- **Today**: Those shift supervisors are probably retired or will be soon; budget cuts have downsized the truck fleet; and the crews are down to one or two veteran workers trying to help much less experienced replacements absorb their 30-40 years of knowledge and experience before they retire – a formidable task, at best. Now, it is becoming increasingly challenging to fill jobs that have already been vacated.

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

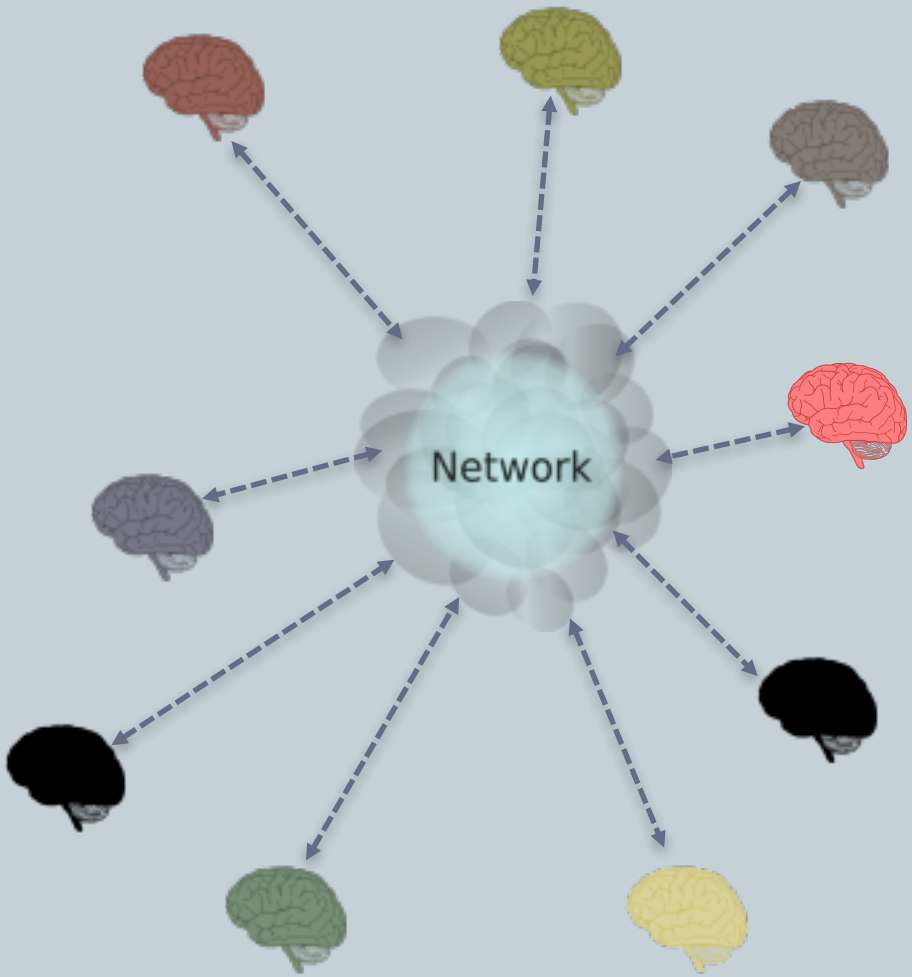
Intelligence That's Built In – Not Bolted On!

There's a Better Way…

This time we have an opportunity to find ways to do things better, faster – and far more efficiently – by replacing those old ideas and processes with tech-centric solutions.

More importantly, we can optimize how we do it, including optimization of the human capital required to achieve key goals and objectives.

In the future, increasingly larger portions of our infrastructure will have a 'brain' embedded for an ever-widening range of purposes.



© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

EXAMPLES OF INTELLIGENT INFRASTRUCTURE

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

EXAMPLE 1: Dams

During most of the 1950s and 1960s, dams were being built in the US at the rate of ~1,000/year…

Most were not equipped with automated monitoring because back then, it was neither practical nor affordable…

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

EXAMPLE 1: Dams…

An industrial computer (e.g., IBM-1800) circa 1968 cost about a million dollars. Today, your handheld smart device has orders of magnitude more power – and for only a few hundred bucks!

Computing power, then…

and now…

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

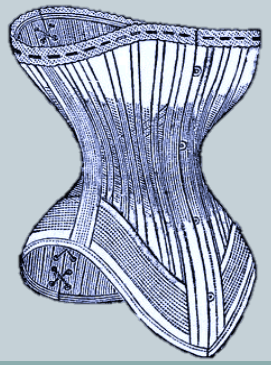
Intelligence That's Built In – Not Bolted On!

EXAMPLE 1: Dams…

Most field data devices ("RTUs") and associated power, sensors and communications were unable to operate reliably in harsh physical environments and cost thousands of dollars…

- ✓ Transducers for vibration and stress (e.g., strain gages) were physically large and very expensive
- ✓ Power supplies were big and bulky and had to be physically wired to the sensors
- ✓ Communications – especially real-time communications – capabilities were very limited with no practical/economical wireless options

In those days, the closest thing to a *'Mesh Network'* looked like this →



© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

EXAMPLE 2: Bridges

The St. Anthony Falls Bridge, the I-35 bridge that replaced the Minneapolis bridge, which collapsed in 2007, was constructed in a joint venture between Flatiron-Manson and Figg Bridge Engineers. Completed in September 2008, the bridge was constructed with two parallel structures, one for each direction of traffic, using pre-stressed concrete box girders. The river span used precast segmental construction and the remaining three spans used cast-in-place concrete.

COLLAPSED I-35 ST. ANTHONY FALLS BRIDGE

>>>

ST. ANTHONY FALLS REPLACEMENT BRIDGE

The total cost for the sensing system was about $1 million, a small fraction of the bridge's $234 million price tag. Over 500 off-the-shelf sensors collect data regarding structural behavior and corrosion on the St. Anthony Falls Bridge.

SOURCES & PHOTO CREDITS: Buildipedia, US Coast Guard

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

EXAMPLE 2: Bridges…

St. Anthony Falls Bridge (continued)…

195 Vibrating Wire Strain Gauges (VWSGs): *Structural deformations are measured by 195 vibrating wire strain gauges (VWSGs), 24 resistive strain gauges, and 12 fiber optic displacement sensors. Temperatures in the bridge and thermal gradients throughout the structure are measured by 243 thermistors, including those integrated into the strain gauges.*

26 Accelerometers: *There are a total of 26 accelerometers measuring modal frequencies of the structure to calculate deflections and structural vibrations. Half of these are installed at the mid-span of each box girder in each span and the other half are located along the exterior box girder of southbound Span 2. These 13, which were installed to collect additional information for future instrumentation, can be oriented in different directions and are uniformly distributed at the corner of the top flange.*

Corrosion Monitoring Sensors: *There are four corrosion sensors included in the deck to determine the susceptibility of the reinforcement to corrosion. These sensors, which are located in the reinforcement strand (a cable wrapped in multiple layers of steel wire), measure the corrosion current, the concrete electrical resistivity, and the concrete temperature to determine the initiation of corrosion, the corrosion rate, water content of concrete, and transport processes of water and chlorides.*

SOURCE & PHOTO CREDITS: Buildipedia

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

INTELLIGENT INFRASTRUCTURE

INDUSTRIES | MARKETS | APPLICATIONS

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

The majority of infrastructure owners/operators fall into six (6) major groups…

- **Energy:** Conventional & Unconventional
- **Utilities:** Electric, Gas, Water, etc.
- **Communications:** Public & Private, Wired & Wireless
- **Transportation:** Land, Sea & Air
- **Government:** Local, State, Federal & Military
- **Facilities:** Buildings & Spaces

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

SOLUTION: Intelligent Infrastructure

Achieving Intelligent Infrastructure involves both short- and long-term measures:

- **Use Existing Tools**: Make better use and application of the vast array of automation tools that already exist and then build on that foundation with integrated Intelligent Infrastructure solutions.
- **Investment Deferrals**: Using existing tools and technologies can defer major investments that would be caused by large-scale replacements. The challenges of infrastructure decline can usually be postponed long enough to develop a more comprehensive long-term solution if appropriate actions are taken.
- **Next Steps**: Designing and building the intelligence in will require more than just advanced technologies and smarter tools. It will have to be compatible with the realities of a very different kind of workforce renewal – one that transitions current managers and workers away from the old ways of doing things and toward newer approaches and solutions.
- **Education Is Key:** We must start now toward building a 21st century workforce that is fully equipped to take on the longer term challenges of Intelligent Infrastructure by design. Tomorrow may be too late…

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

Some Ways to Advance Intelligent Infrastructure

TARGET GROUP	Strategies, Tactics, Actions
EVERYONE	• Educate yourself about Intelligent Infrastructure and share your knowledge. • Talk with management, peers and employees about how your infrastructure can be made more intelligent, starting at the planning and design stages. • Create articles, white papers, webinars and workshops around Intelligent Infrastructure concepts for internal and, where applicable, external use.
INFRASTRUCTURE SUPPLIERS & CONSULTANTS	• Present seminars, webinars & workshops for your clients/customers to educate them about Intelligent Infrastructure. • Incorporate Intelligent Infrastructure into your sales and marketing strategy • Partner with clients/customers to explore and exploit synergies resulting from a strategic shift toward Intelligent Infrastructure.
INFRASTRUCTURE OWNERS/ OPERATORS	• Create a task force or working group to study ways that Intelligent Infrastructure can help achieve corporate goals, address KPIs, and improve top and bottom line. • Become a Thought Leader in your market/industry by demonstrating the need for and purpose of Intelligent Infrastructure in a real-world context • Incorporate Intelligent Infrastructure into your Technology Strategy Plan (TSP) – and if you don't have a TSP, create one!

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED

The Case for Intelligent Infrastructure

Intelligence That's Built In – Not Bolted On!

THANK YOU!

QUESTIONS?

mam@InfoNetrix.com

T: +1 504-466-2220

POST OFFICE BOX 641177 | KENNER LOUISIANA 70064-1177 USA

© 2016 INFONETRIX LLC ALL RUGHTS RESERVED