

PREDIX

Performance and Cyber Security in the Industrial Internet: Two Sides of the Same Coin



Introduction

The Industrial Internet of Things (IIoT) represents a huge opportunity for growth and efficiency for companies across industries. By using intelligence in machines and the information that can be gained from them, enterprises and organizations will be able to get far more efficiency out of their assets and their markets. Valuable operational and business insights from IIoT will trigger ideas for smarter configuration and deployment, accelerated time-to-value, and new service-oriented revenue streams. With investment in infrastructure assets expected to top \$60 trillion over the next 15 years¹, for many large-scale industries, even a 1% increase in efficiency due to the Industrial Internet could yield tens of billions of dollars in savings.

Even a 1% increase in efficiency due to the Industrial Internet could yield tens of billions of dollars in savings.

Underpinning all of this potential is data—big data. Machines can generate data about their status, activity, and performance every day, hour, minute, or second. IIoT is already generating data twice as quickly as any other sector. To reap the benefits of this massive resource requires solutions with enough performance to handle countless real-time data flows to monitor machines, analyze events, and control actions. Two halves of the IIoT must work together: information technology (IT) to initiate industrial outcomes and operational technology (OT) to put them into effect.

In order for industries to harness the power of the Industrial Internet, the vital topic of cyber security must also be addressed. Cyber security is a top concern regarding the Industrial Internet, and for good reason. The industrial world is full of operational technology based on critical physical assets and machinery. Historically, the world of OT was not built for wide Internet access or with modern security risks in mind. To compound the problem, performance and cyber security have often been viewed as “either-or,” with gains in one area forcing sacrifices in the other.

This white paper provides an overview of the opportunity associated with the Industrial Internet and the threats it faces. If performance and security are truly to be two sides of the same coin—scaling together positively as enterprises increase their use of intelligent machines and industrial big data—a fresh approach to security is required.

Following an examination of the comprehensive security strategy required by the Industrial Internet, this paper then examines how GE's Predix cloud platform for the Industrial Internet, and OT system environments fights against cyber attacks.

In order for industries to harness the power of the Industrial Internet, the vital topic of cyber security must also be addressed.

¹Press release, “GE Announces Predix Cloud - The World's First Cloud Service Built For Industrial Data And Analytics,” August 5, 2015
<https://www.ge.com/digital/press-releases/GE-Announces-Predix-Cloud-Worlds-First-Cloud-Service-Built-Industrial-Data-Analytics>






What if... Potential Performance Gains in Key Sectors				
Industry	Segment	Type of Savings	Estimated Value Over 15 Years (Bil- lion nominal U.S. dollars)	
 Aviation	Commercial	1% Fuel Savings	\$30B	
 Power	Gas-fired Generation	1% Fuel Savings	\$66B	
 Healthcare	System-wite	1% Reduction in System Inefficiency	\$63B	
 Transportation	Freight	1% Reduction in System Inefficiency	\$27B	
 Oil & Gas	Exploration & Development	1% Reduction in Capital Expenditure	\$90B	

Table 1. Industrial Internet: The Power of 1%

The Industrial Internet opportunity

At the center of the Industrial Internet are cyber-physical systems, which the National Institute of Standards and Technology (NIST) defines as “co-engineered interacting networks of physical and computational components.” According to NIST, “These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas. Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management, and electric power generation and delivery, as well as in many other areas now just being envisioned.”²

The practical advantages offered to users are numerous. By connecting intelligent machines, big data analytics, and data-empowered workers, the Industrial Internet can reduce unplanned downtime and open up new opportunities for growth. Sensors on machinery can provide real-time performance information that can help identify problems before they occur. Big data analytics can create an aggregate view across machines, components, and systems, providing insight into real-time operations. As an example, RasGas, one of the world’s premier integrated Liquefied Natural Gas (LNG) enterprises, is using IoT-powered predictive maintenance to extend the life of its assets and lower operating costs through greater efficiencies. Insights into plant operations are enabling forward-looking decisions that improve business operations.³

Using the Industrial IoT in this way, more work gets done with less effort, and assets run more predictably. Enterprises move from a reactive “break-fix” approach to proactive problem prevention, decreasing unplanned downtime and increasing asset lifespan. Product-centric business models are extended to or replaced by more lucrative service-based offerings, with the flexibility and responsiveness to meet fluctuating business demands.

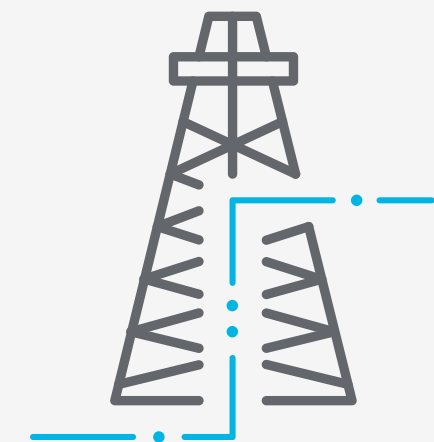
Data is the key enabler for all the benefits and opportunities that come with the Industrial Internet. Its potential for constructive use by organizations for their own benefit and that of their customers and communities is huge, but so is its potential for misuse in the wrong hands. With critical industrial equipment and services at stake, the need for excellence and robustness in data and asset security is urgent.

Transforming an oil field

When you look at a typical oil field with all its pumps, the vast majority of the data associated with those pumps is right at the control system on the pump itself. Typically, that data is not centrally collected. To find out what is happening with all those pumps—including even the most basic information of whether they are running or not—requires a person in a pickup truck driving around the oil field and noting any pumps that appear to be having problems. Later a technician will be dispatched to fix that pump.

Although this case sounds simple, the cost of doing business this way is substantial. It could take as long as three weeks just to find out that a particular pump is down, which means three weeks of lost production and millions of dollars lost.

The Industrial Internet can transform this situation by collecting data from each pump and sending it to a cloud-based environment. The company has a dashboard to manage the pumps in the oil field. They are able not only to see which pumps are running but also to determine the performance of the pumps and decide whether to run all of them or a subset based on current yields.



² NIST, Cyber-Physical Systems Homepage, Cyber-Physical Systems Homepage, <http://www.nist.gov/cps/>

³ GE Power, “The Cloud Advantage: Six Reasons Power Leaders Are Moving to Cloud,” p. 6. https://www.predix.com/sites/default/files/the_cloud_advantage_120315_final.pdf

Cyber security threats and challenges

The cyber security threats that come with a connected industrial world are challenging because of the sensitive areas in which the industrial world operates. OT infrastructure is mission-critical, and has implications for the safety, security, confidentiality, availability, and privacy of society at large. Airplane components, electric grid assets, and hospital equipment are cases in point. Whereas in conventional IT, attackers target personal information or intellectual property, attackers in the OT world go further and attack entire operational processes.

The greatest threat to the OT infrastructure, in this regard, is service disruption or harmful impact to critical infrastructure. If attackers seek to shut down processes, they can put public health, safety, or national economic security in peril.

Industrial machines also have unique “attack surfaces.” They are vulnerable to environmental threats such as electromagnetic pulses, power interruption, atmospheric variations, and extreme temperatures, all of which can menace critical machines and their operations if exploited by attackers, criminals, or other bad actors.

Such threats are not far-fetched. Industrial control systems are already showing their vulnerability to attack: a recent survey by SANS found that 32% of respondents believed that their control system assets or networks had been infiltrated or infected at some point, and 34% believed that their systems were breached more than twice in the past year.⁴ Part of the problem is that even newer sensors and devices (the “things” of the Internet of Things) are often designed without proactive planning for security. This makes them vulnerable to malware as well as other types of attacks.

Contrary to popular belief, OT does not have to be connected to the Internet at large to be at risk. OT organizations often assume that because their systems are “air gapped” (that is, not connected to the Internet), those systems are not susceptible to security threats. However, this assumption is wrong. Operational systems are increasingly being exposed to risk, be it via a thumb drive or a misconfiguration by a well-intentioned employee.

Companies must consider how to secure OT given these different challenges so that they are both protected now and well-positioned to take advantage of increased performance, productivity, and profitability from the Industrial Internet.

Securing OT is not easy. Operational equipment is a mash-up of old and new technology. Much of the machinery and operational technology in use today was put into service before Internet connectivity became widespread. Adding Internet connectivity (an IP interface) to existing systems can create unforeseen attack vectors. Not only that, but existing IT security solutions simply won’t work in the OT environment. OT consists of many proprietary hardware and software systems that use unique protocols. A traditional IT solution does not understand the OT protocols, processes, and commands, and therefore cannot protect OT processes.

Nonetheless, businesses must find a way to press forward with the Industrial Internet opportunity without exposing their companies to risk. Failure to act is not an option. Businesses that do not begin to securely adapt to the digital industrial era will face an entirely different sort of threat: that of falling behind.

If attackers seek to shut down processes, they can put public health, safety, or national economic security in peril.



⁴ SANS Institute, “The State of Security in Control Systems Today,” June 2015.

<https://www.sans.org/reading-room/whitepapers/analyst/state-security-control-systems-today-36042>

A security strategy for the Industrial Internet

Companies need a strategy for adopting security that better positions them to take advantage of the opportunities presented by the Industrial Internet. They need a way to effectively bridge the worlds of IT and OT in a manner that can establish end-to-end security and trust—from the factory floor to users on their devices.

Traditionally, IT security has involved adding an extra layer of protection, after an IT product or system has been developed. When all those systems were located on an organization's own premises, the strategy was then typically to apply security over and around them. Performance and security ended up as antagonists with performance struggling to break limits and security attempting to impose them. However, the Industrial Internet exists outside of a corporation's perimeter and security cannot simply be layered over it.

The answer is to design for performance and security so that they work with each other, not against each other, and scale easily and reliably, as the use of machine intelligence and industrial big data grows.

GE, a leader in the Industrial Internet, has developed a comprehensive cyber security strategy from which to develop such a design, based on four key pillars:

- Secure and certify the operational systems environment
- Bridge IT and OT security
- Enable development of secure Industrial Internet applications at scale
- Drive security to the user and device level





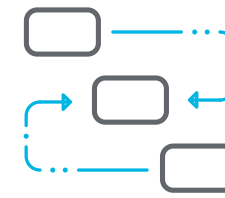
PILLAR 1: Secure and certify the operational systems environment

The cyber-physical systems that comprise controllers, sensors, industrial software, and industrial networks are exposed to threats at many levels, including EMI/EFI, power, atmospheric, and thermal, as well as software and hardware.

The first step in combating these unique threats is to assess machine and operational systems and certify that they meet a comprehensive set of requirements or industry recognized security assessment and certification standards, such as ISO 27001/2, ISA/IEC 62443, or NIST 800-53.⁵ An in-depth evaluation of devices should identify vulnerabilities and provide mitigation recommendations to address weaknesses that could be exploited. Given the difficulty of securing industrial control systems (ICS) and SCADA network devices in deployment, security assessments should be conducted throughout the development lifecycle. Ideally, weaknesses will be discovered—and mitigated—before devices are deployed in the field.

Second, and perhaps more critically, the processes that transpire across devices, applications, and protocols in an OT environment need to be monitored and controlled. This task is difficult because most environments have a vast array of vendors, devices, software, and protocols, all on different change and patch management cycles.

Traditional security technologies like firewalls that attempt to separate a company from the outside world do not provide the kind of protection needed for these environments. Although useful for protecting data coming to or from the IT environment (such as sensor or optimization data), expecting a firewall to provide visibility or protection within an OT environment is like expecting automobile brakes to stop an airplane. The end goal is the same (control or prevent motion in this example), but the design, architecture, and operational risk premises are entirely different. Security is needed at every layer in order to be effective.



PILLAR 2: Bridge OT and IT security

Once operational infrastructure is secured from OT-specific threats, the challenge becomes to securely bridge OT with IT big data technologies that will help unleash the power of the Industrial Internet.

Trusted connections must be established from OT to IT and to the cloud, and organizations must have visibility into their information assets in these mixed environments. And as more machine data enters the IT analytics infrastructure, security professionals, used to reviewing smaller logs generated by software, need to be prepared to secure larger volumes of data.

Bridging OT and IT has another strong requirement: cyber security must not be intrusive to the OT environment. Unlike the enterprise IT world, where the user experience is sometimes sacrificed in the interest of reducing risk, cyber security must have minimal impact on operations. A large part of

keeping IT systems secure involves patching them as new vulnerabilities are discovered. This procedure does not carry over well to the OT world, where regular maintenance windows do not exist to support updating systems with the latest patches.

Downtime in OT means a lack of productivity and financial losses, which can add up to millions of dollars per day. Properly secured OT requires that organizations make system changes less frequently in order to minimize the impact on operations, whether the goal of those changes is to optimize performance in response to operational data or to secure an application.

⁵ Details about ISO 27001/2 and ISA/IEC 62443 can be found at https://en.wikipedia.org/wiki/Cyber_security_standards
For NIST 800-53, see https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53



PILLAR 3: **Enable development of secure Industrial Internet applications**

An essential element for generating meaningful insight from industrial big data analytics is the development of Industrial Internet applications. Just as they have already been for consumer Internet and mobile technology, apps will be a major mechanism for innovation in the Industrial Internet space.

Apps designed to optimize OT environments will provide useful real-time insights, controls, and ways to optimize production. However, apps can also harbor security threats. Industrial Internet apps need to be able to continuously deliver new functionality while simultaneously providing top-tier assurance for data privacy and security. This requires the creation of app factories that include everything needed to expose any threats inherent in the use case and help to reduce them without impact on developer productivity. Safety, security, scalability, reliability, and manageability must be built into the tools developers use. Data governance also must be built in and integrated across the app factory. A matrix of complex regulation and compliance checks must be served up as part of the total solution.



PILLAR 4: **Drive security to the user and device level**

The final pillar is the secure extension of Industrial Internet apps to enterprise end users. It is vital that machine and data security be preserved at the end-user level while still providing robust functionality. It is also likely that end-users will not be IT experts (even if they are OT experts).

The design of Industrial Internet apps, therefore, must meet consumer-grade expectations of usability—without compromising security. Authentication, verifying the identity of the user, and authorization, determining the privileges a particular user has, must be simultaneously robust and flexible, adapting to user roles and responsibilities without exposing security risks. On top of that, organizations must maintain an end-to-end chain of custody for all data so that they can enable user interactions that drive value to operations and protection to equipment.



GE powers the Industrial Internet through cyber security technology

GE Digital has already applied its four-pillar strategy for its own requirements to create a secure backbone for the Industrial Internet. It serves as an example of how to build security into Industrial Internet architecture.

To secure and certify operational infrastructures, GE developed GE Digital Cyber Security, a division specializing in security for control systems and operational technology. For industrial data, GE Digital developed Predix, a distributed application and services platform purpose-built to develop and deploy industrial asset performance management and operations optimization applications with reliable governance and cyber security controls.

GE Digital Cyber Security is one of the few organizations equipped to help companies harden OT systems against the increased risk of cyber attacks as they connect their assets.

Securing operational system environments

Most OT infrastructures were not designed for broad connectivity to IT systems that consume operational and sensor data. The core value of GE Digital's cyber security is its unique knowledge and approach to thoroughly investigating the embedded aspects of machine security, such as physical, electro-mechanical, RFI, EMI, and power-line attacks, alongside attacks on operational firmware and sensor elements. This approach, combined with field security assessments for operational environments and factories, makes GE Digital one of the few organizations equipped to help companies harden their OT systems against increased risk of cyber attacks as they connect their assets.

GE Digital's cyber security portfolio centers on OpShield, a solution designed to provide policy-driven security for complex multi-vendor OT system environments. This solution provides ongoing protection from emerging threats while minimizing disruption or downtime for OT equipment.

GE Digital's Achilles certification processes and technology are used to create a catalog of trusted machines and environments, helping to enable connected industrial environments. The cyber security certifications include Achilles Communication Certification (ACC), which entails network assessment of each device against standard attacks, and Achilles Practices Certification (APC), offering security policy and practices audits to help operators adhere to international standards, such as IEC 62443-2-4.⁶

GE Digital's industrial-grade services and solutions help reduce the attack surface and protect automated connectivity of operational systems. The solution also secures the flow of Industrial Internet information with a common data awareness and governance stack, using a data architecture that extends from the operational systems all the way to end-user applications.

⁶For a detailed presentation, see "Achilles Assurance Platform" available at https://ics-cert.us-cert.gov/sites/default/files/pcsf-arc/achilles_assurance_platform-kube.pdf

Securing Operations Optimization: Predix

Predix is a purpose-built industrial cloud designed to securely connect with multiple machines, old and new, from different vendors on very large industrial scales. Predix manages a heterogeneous mix of data and communications protocols to aggregate information from all of these devices. The design behind Predix offers a glimpse into how to address the data concerns of the Industrial Internet.

Predix is a purpose built industrial edge-to-cloud platform designed to securely connect with multiple machines, old and new, from different vendors at scale.

Governance and certifications

Governance and certifications are essential components of an Industrial Internet platform that deals with sensitive information and high-stakes industries. Predix builds in governance from the end-user right through to the operational infrastructure. Instead of layering governance and certification onto existing IT data workflows, Predix integrates them directly into its architecture.

Predix is built on a common infrastructure governance model based on ISO 27001/2, NIST 800-53, and FIPS 140-2 to manage the availability, integrity, and security of enterprise data. The platform also leverages common controls that support compliance with more than 60 national, international, and governing body regulations, meeting or exceeding the requirements of customers from a very broad range of industry sectors.

Platform hardening

When evaluating cloud technology, industrial companies are frequently concerned about levels of accountability and visibility into the proper functioning of the system. If a problem occurs, it is essential to have clarity on what went wrong, where, and how to fix it. To that end, GE has implemented platform hardening at every layer within Predix.

Privileged access and identity management

Privileged identity management, object and device identification, and granular developer access controls offer a defense-in-depth view of all actors within and around Predix. In parallel, security features like client-side token validation significantly improve performance by eliminating extra network roundtrips.

App factories

Enterprise app factories and developer communities that provide operations functionality play a key role in establishing a secure software development ecosystem. However, application development security cannot be left to chance or to the expertise of each developer, especially since many are from the IT world seeking to drive OT benefits, but are unfamiliar with industry. Therefore, security, governance, and privacy cyber protections have been built into Predix integration and deployment systems, without direct impact on the developer or the application.

The Predix infrastructure team follows a complete “DevOpsSec” (development-operations-security) process for all apps and microservices created by developers in the app factory. As part of DevOpsSec, Predix makes tools available to help developers create secure workflows, handle data properly, evaluate app users, and dynamically test applications and APIs prior to deployment. This includes the ability to establish baseline performance and highlight potential security holes.

By combining DevOpsSec with static and dynamic automated testing, Predix helps keep new code as clean as possible. Predix can also survey new microservices arriving into the development area to detect any abnormal or suspicious behavior. This approach greatly reduces the possibility of malware making its way into the Predix runtime environment.

User-based world

The customizability and configurability of apps in the consumer world is now extending to the industrial world. But if end-users can tailor applications, sometimes in ways not conceived of by the developer, absolute visibility is required. Predix achieves this through continuous monitoring at every layer, with data loss protection and malware detection from the external networks to the execution point of the application instance or microservice.

This visibility extends into the exchanges to/from the OT environment and creates a “heat-map” dashboard for the Predix security operations team to protect customers served by Predix. Also, the Predix team provides guidance for the shared responsibility of the user organization to implement controls at the application and data layers.

Predix innovations in cyber-info-ops security

Using a PaaS solution and a common runtime structure that is elastic for all applications creates opportunities for cutting-edge improvements in security. The Predix platform delivers several key innovations.

Individual app/user visibility

Predix is built on Cloud Foundry open source technology and provides secured multi-tenancy capability. Apps that run in the Cloud Foundry environment are separated from operational and control elements in the network. This means that an app can be scaled by running multiple instances of it, with each instance optimized for security and performance.

Predix can monitor the user and application interactions between each specific app instance and user—in and out of the Internet and through all the services. By leveraging a combination of software defined network (SDN) technology and integrated content inspection, Predix can pinpoint suspicious behaviors and eliminate them as necessary.

Isolation of rogue actors and actions

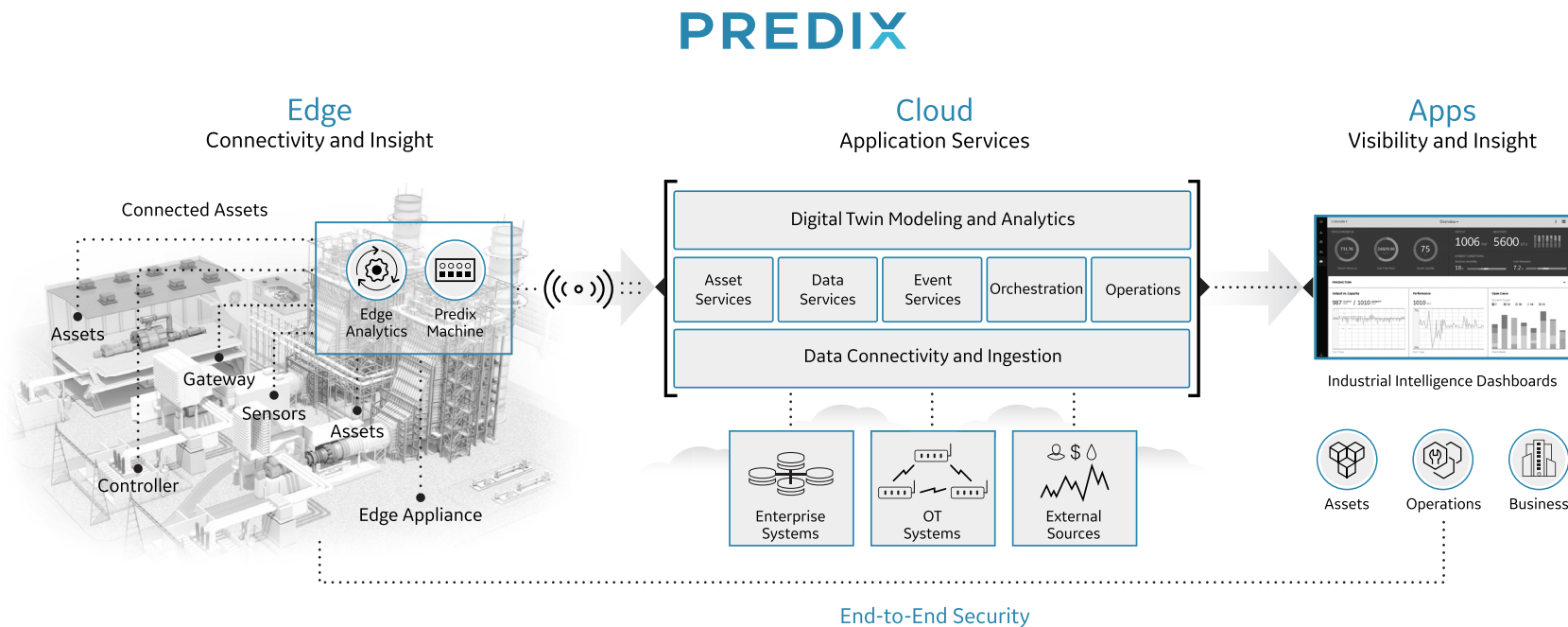
Predix can also restructure the soft network fabric in its SDNs. Information gained from app and user visibility enables Predix to isolate activities and monitor them, separating them from critical data flows and avoiding impact on the rest of the Cloud Foundry infrastructure.

Integrated identity vetting and proofing

As developers use Predix to develop and catalog services, their identity is independently validated. Predix uses national and international information validation services to make sure a developer’s identity is established and revalidated as required. Developers are also required to undergo a proofing verification process that asks for information only the right person could know. Over the lifecycle of the developer’s activities, the level of vetting can be increased to check on any changes in the developer’s persona.

Enhanced security controls

The Predix cloud has security embedded at every level of the cloud stack. This specialized approach offers industrial-grade security as every layer is monitored and scanned for vulnerabilities. Capabilities include encryption, key management, incident response services, logging, network-level security, support for end-to-end chain-of-custody reporting for code and data, and a 24/7 security operations center.



Conclusion

The Industrial Internet offers tremendous opportunity to optimize and drive performance of industrial machines, but performance must go hand-in-hand with cyber security. With Predix, performance and security are two sides of the same coin. Enterprises and organizations benefit from powerful performance in tandem with a security approach that secures OT, IT, and applications so that they can confidently execute their Industrial Internet strategy.

GE Digital has developed an end-to-end approach to cyber, information, and operational security that establishes the trust and visibility required for the Industrial Internet. GE Digital's four-pillar approach ensures that both old and new OT infrastructure is protected against a variety of evolving threats, while also securing IT infrastructure and applications. Complete visibility and continuous monitoring ensure that the environment remains secure even as it grows in scope and scale. In conclusion, GE Digital effectively addresses security across environments to enable industrial companies to safely realize the tremendous potential of the Industrial Internet.

Complete visibility and continuous monitoring ensure that the environment remains secure even as it grows in scope and scale.



Learn more

The Predix Catalog also serves as a marketplace for third-party IIoT services and analytics. A sampling of the many Catalog offerings provided by third parties appears below.

Intelligent Environments	Geospatial	Operations	Analytics
<p><u>Traffic planning</u></p> <p>Optimize operations & planning with vehicle traffic data.</p> <p>—Current</p>	<p><u>Location Intelligence</u></p> <p>Optimize operations & planning with vehicle traffic data.</p> <p>—Pitney Bowes</p>	<p><u>Logging</u></p> <p>Manage all your app logs and save, search, and visualize them.</p> <p>—Logstash</p>	<p><u>Statistical Methods and Analysis—Kalman Filter</u></p> <p>Filters noise in data and provides smooth signal.</p> <p>—GE Transportation</p>
<p><u>Parking planning</u></p> <p>Optimize operations and planning with vehicle parking data.</p> <p>—Current</p>	<p><u>Dynamic Mapping</u></p> <p>Enhance your asset data by recording the current and historical locations of moving assets.</p> <p>—GE Energy Connections</p>	<p><u>Machine Data Analytics</u></p> <p>Simplify collection and analysis of big data from infrastructure, security systems, and business applications.</p> <p>—Splunk</p>	<p><u>Event Stream Processing</u></p> <p>Analyze continuously flowing data over long periods of time where low-latency incremental results are important.</p> <p>—SAS</p>
<p><u>Situational Awareness</u></p> <p>Obtain media such as photos and video to enhance safety awareness.</p> <p>—Current</p>	<p><u>Intelligent Mapping</u></p> <p>Enhance your asset and analytical data by visualizing and aggregating the data on a map.</p> <p>—GE Energy Connections</p>	<p><u>Business Operations</u></p> <p>Measure and monetize your service with subscription management, entitlements control, metering, and revenue management.</p> <p>—Nurego</p>	<p><u>Anomaly Detection</u></p> <p>Use this standalone analytic service to identify threats and anomalous events in critical infrastructure and operations.</p> <p>—Thetaray</p>
<p><u>Indoor Positioning</u></p> <p>Capture mobile device indoor locations with 10cm accuracy.</p> <p>—Current</p>			<p><u>SKLearn Machine Learning Invoker</u></p> <p>This analytic wraps the Python machine learning package for use in the Predix Analytics Library.</p>

Learn More: See the complete Predix [Catalog of Services](#) and [Catalog of Analytics](#). Visit www.predix.io to access our full catalog of microservices.



About Predix

Predix is the Industrial Internet platform that connects data from physical assets to powerful analytics. Predix can operate everywhere industry does, allowing companies to quickly and securely connect their assets, collect data, and build and run applications.

ge.com/digital/predix
predix.io

© 2017 General Electric Company—All rights reserved.

GE, the GE Monogram and Predix are trademarks of General Electric Company.

No part of this document may be distributed, reproduced or posted without the express written permission of General Electric Company.

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED “AS IS,” WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

02 2016

