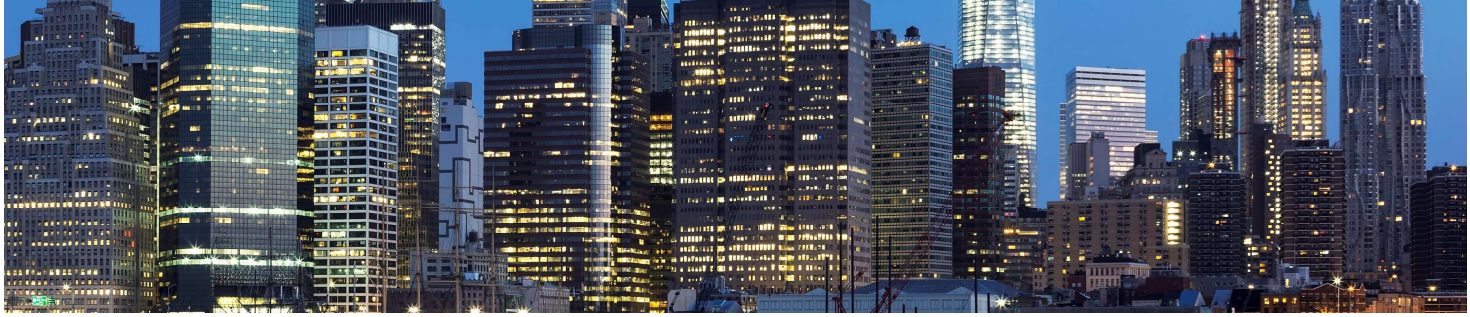
SIGA
Level Zero OT Resilience

# Industry 4.0 - The Digital Transformation of urban transport

December 2022



# Background

A public benefit corporation responsible for public transportation, is the largest public transit authority in the United States, serving 12 counties in in North America, carrying over 11 million passengers on an average weekday systemwide, and over 850,000 vehicles on its seven toll bridges and two tunnels per weekday.

The network comprises the nation's largest bus fleet and more subway and commuter rail cars than all other U.S. transit systems combined.

# The challenge

## How Do You Know Which Sensors, Controllers and OT Devices are Vulnerable?

- Transportation and logistics operational environments contain thousands of devices from multiple vendors. For example, assets that track equipment performance, humidity and luminosity are used in passenger and luggage screening systems, environmental and lighting controls, and so much more.
- Protecting underground utility tunnels from invisible dangers. These tunnels, particularly those used for the transportation, such as HVAC systems and water level, present specific hazards because of flammable or toxic gas leaks, oxygen deficiency, overheated cables, and smoldering electrical fires. A fire or gas leak in these areas can lead to catastrophic consequences and cost millions of dollars in disruptions and lost business.
- Unfortunately, most operational devices lack the built-in security required to keep passengers, data and systems safe.
- Data from devices and processes need to be available for analysis that informs decisions and drives operational efficiencies. However historically, OT systems and devices have been designed with isolation in mind — not to connect and communicate with IT systems and the internet.
- Visibility. Response and remediation of system failures is difficult because the rail operator has zero visibility into their industrial networks

# The solution

## *Prevent Transportation & Logistics Operational Disruption*

SIGA OT Solutions tackles the risk of transportation and logistics system downtime through assets monitoring and anomaly detection that alerts you to irregular behavior.

## Baselining Variables

In the initial learning phase, the solution uses machine learning and artificial intelligence to observe IOP and create asset and operational baselines. It models behavior and correlates multiple types of data, including information about similar assets within the system, to determine what normal activity looks like.

## Detecting Anomalies

In monitoring phase, the solution automatically detects when a specific device or automated operation is deviating from its baseline and moving towards a state that could disrupt services. It uses advanced correlation and context to deliver a simple, consolidated view of what's happening, and proactively alert that remediation may be necessary.

Anomaly detection significantly reduces troubleshooting efforts and enables to take action before a device or automated operation fails.

# SIGA's unparalleled offering

To secure their expansive, heterogenous OT environment and safely connect with IT systems, the rail operator selected SIGA OT Solutions as its partner, utilizing the following solutions SIGA develops:

# SigaGuard

An Out-of-Band, cyber security solution for Operational Technology (OT) environments. Equipped with forefront technology, SigaGuard is the only solution that protects mission critical machinery and processes from Level 0.

**Autonomous:** Detached from IT networks, SigaGuard is a Plug & Play solution allowing remote monitoring completely agnostic to the ICS platform.

**Reliable:** Gain visibility of the deepest source of unfiltered and un-hackable data by monitoring electrical signals at the physical layer (Level 0)

**Smart:** Advanced Machine Learning and Artificial Intelligence algorithms detect cyber and operational anomalies and deliver actionable insights.

# SigaGuard Parallel Reference Monitoring (PRM)

The PRM system conducts a constant comparison between the data packets reaching the PLC and the information coming from the electrical signals to SigaGuard. SIGA's PRM add-on detects cyberattacks such as Stuxnet in a matter of second and reports about them instantly.

The PRM add-on was developed to compare between what appears in the HMI to what actually happens below the surface, at Level 0. This comparison prevents attacks such as HMI Spoofing, as the PRM add-on provides operators with constant visualization into Level 0, ensuring operators have the upper hand in case of a cyber-attack.

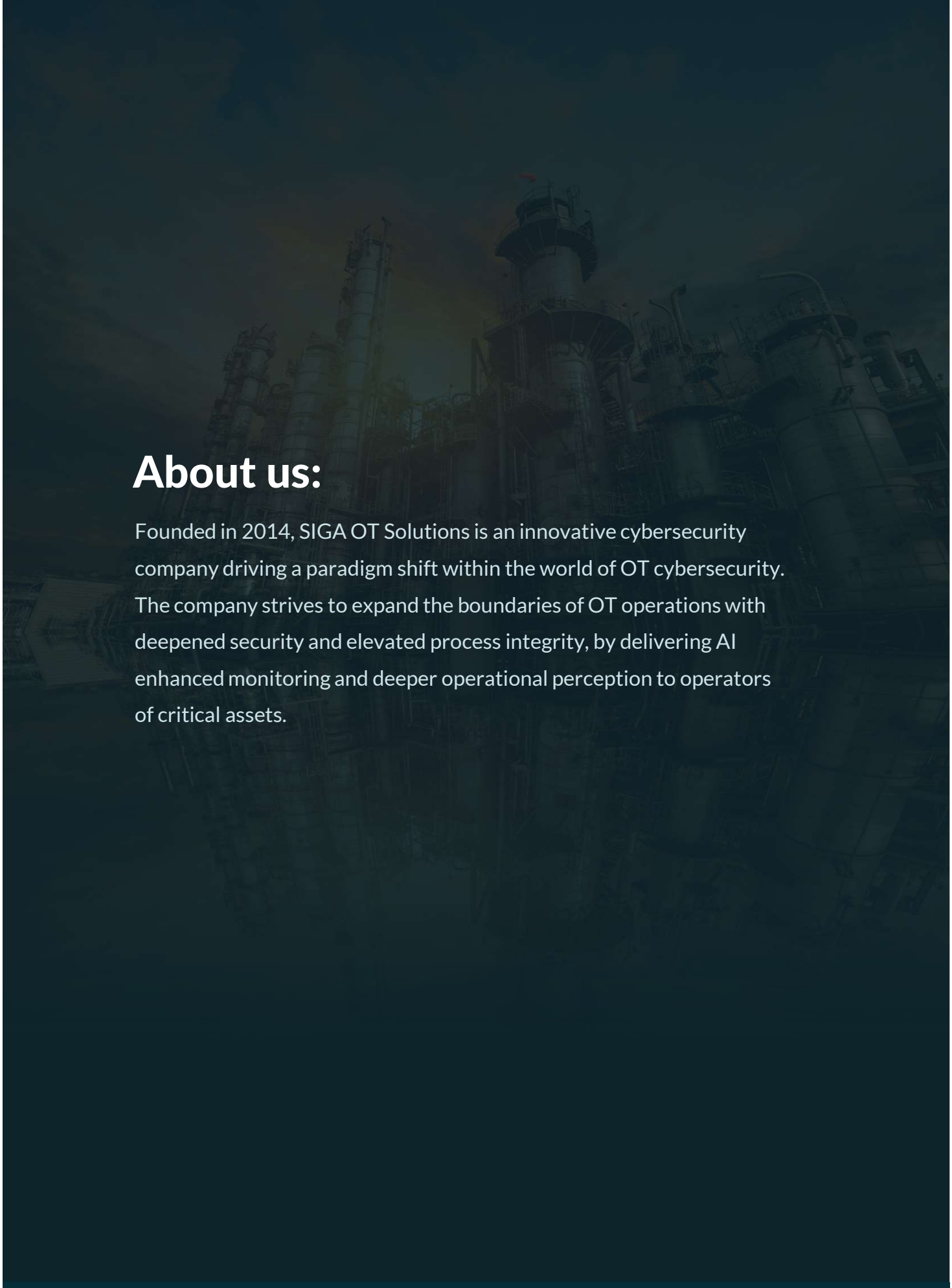
# Outcomes

Full visibility and asset profiling to understand exposure to cyber risk. The rail operator has telemetry and, visibility to quickly determine if suspicious activity is happening on any of their OT networks or devices – even in aging systems that utilize proprietary protocols. They can monitor for threats and identify risks, allowing them to act faster to mitigate risk and assure continued operations of critical processes.

# Voices of the customer

We have been widely impressed with SIGA's novel approach to operational process monitoring and Cybersecurity in OT environments. SIGA has a dynamic, enthusiastic and highly motivated team, with a great vision, hence, we are excited to fuel this collaboration and aim for fruitful results.

ICS and operational processes are at the core of our organization. The fact that SIGA has developed solutions that generate actionable insights directly from the source, could become an enabler for us to introduce a variety of new industry 4.0 solutions to our global business.



# About us:

Founded in 2014, SIGA OT Solutions is an innovative cybersecurity company driving a paradigm shift within the world of OT cybersecurity. The company strives to expand the boundaries of OT operations with deepened security and elevated process integrity, by delivering AI enhanced monitoring and deeper operational perception to operators of critical assets.