SIGA
Level Zero OT Resilience

Chemical

Production Plant

Elevating OT cybersecurity to Level 0

The client

A Global Chemicals Manufacturing Company

A chemical production plant in Israel. SIGA monitored 2 chemical process manufacturing lines.
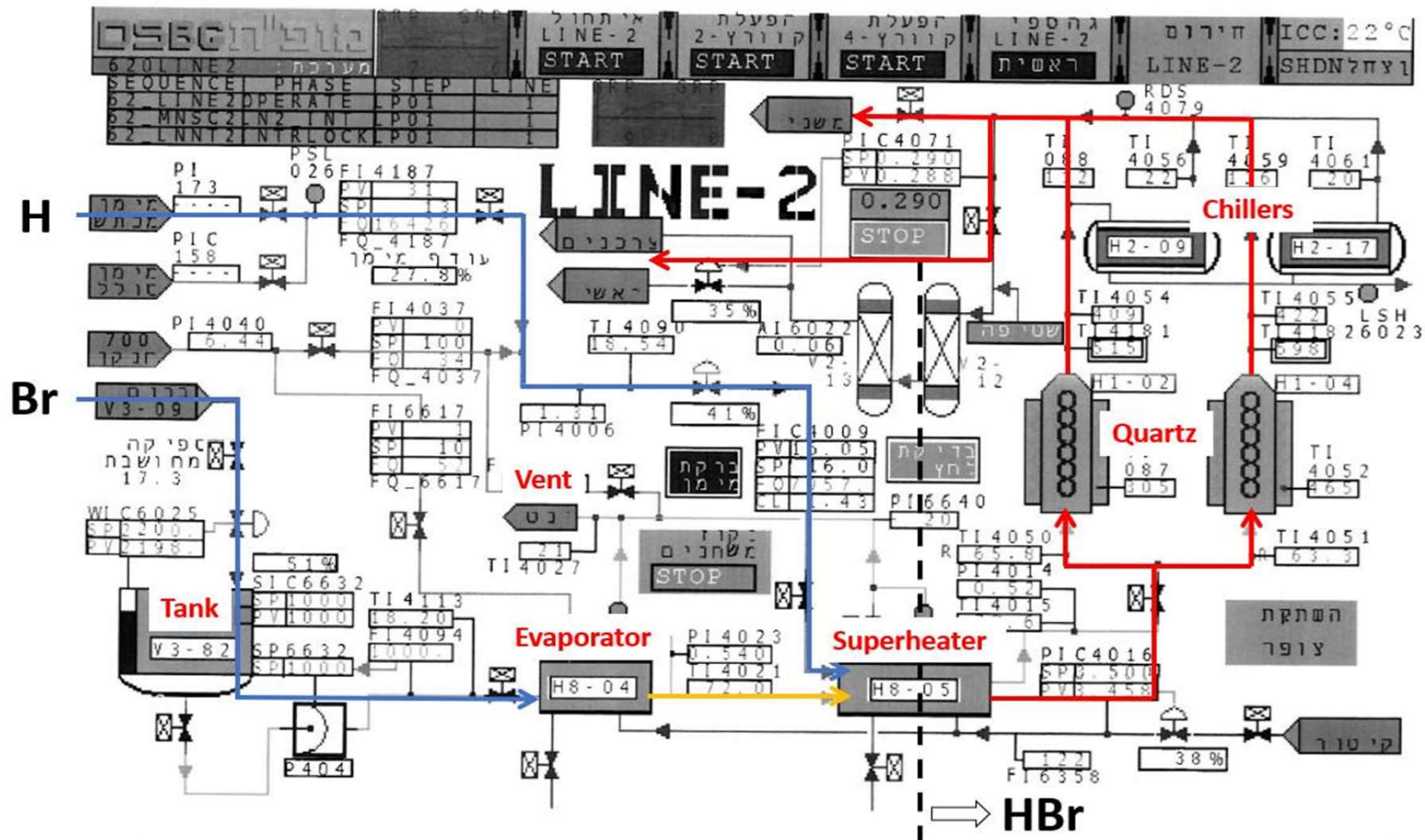
SIGA
Level Zero OT Resilience

The challenge

- The organization's chemical processing production lines run 24/7. The lines suffered from occasional unintended failures which led to continuous shutdowns, due to sudden and abrupt malfunctions.

- These failures led to accumulative downtime and financial losses (roughly 150K$ per day), on top of other functional issues stemming from the same failures.

- The built-in ICS and control measures were not providing early warnings prior to the process's shutdown.

- The plants' engineers were struggling to figure out what causes these failures.

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

The Process Description

The solution

SigaGuard provides ultimate granular process visibility delivering the most reliable insights coming directly from the electrical signals at Level 0.

By reporting to the engineers of malfunctions to the process in real-time, downtimes can be reduced to a minimum and even be prevented.
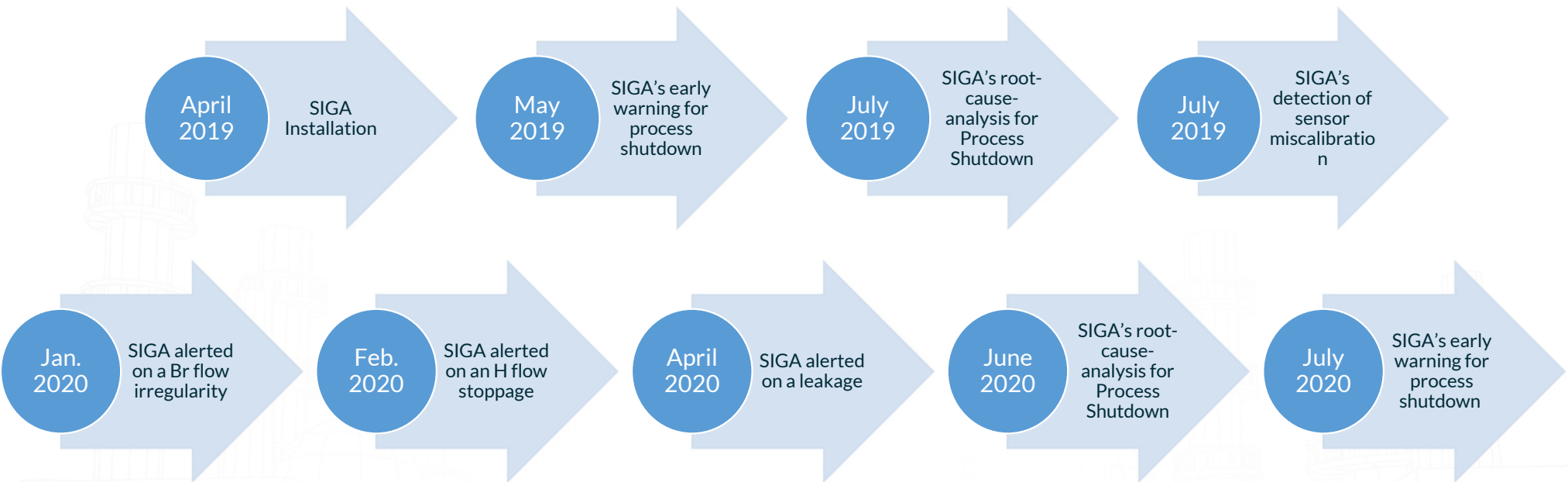
SigaGuard is an out-of-band solution which ensures that the operators can feel the machinery's pulse and act upon the threats quickly and efficiently to protect and improve critical processes.

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

Installation Phase

- Two days of installation and integration were conducted in April 2019

- Monitoring 54 IOs (48 Analogue, 6 Discrete)

Use Case Events Log

April 2019 — SIGA Installation

May 2019 — SIGA's early warning for process shutdown

July 2019 — SIGA's root-cause-analysis for Process Shutdown

July 2019 — SIGA's detection of sensor miscalibration

Jan. 2020 — SIGA alerted on a Br flow irregularity

Feb. 2020 — SIGA alerted on an H flow stoppage

April 2020 — SIGA alerted on a leakage

June 2020 — SIGA's root-cause-analysis for Process Shutdown

July 2020 — SIGA's early warning for process shutdown

SIGA
Level Zero OT Resilience

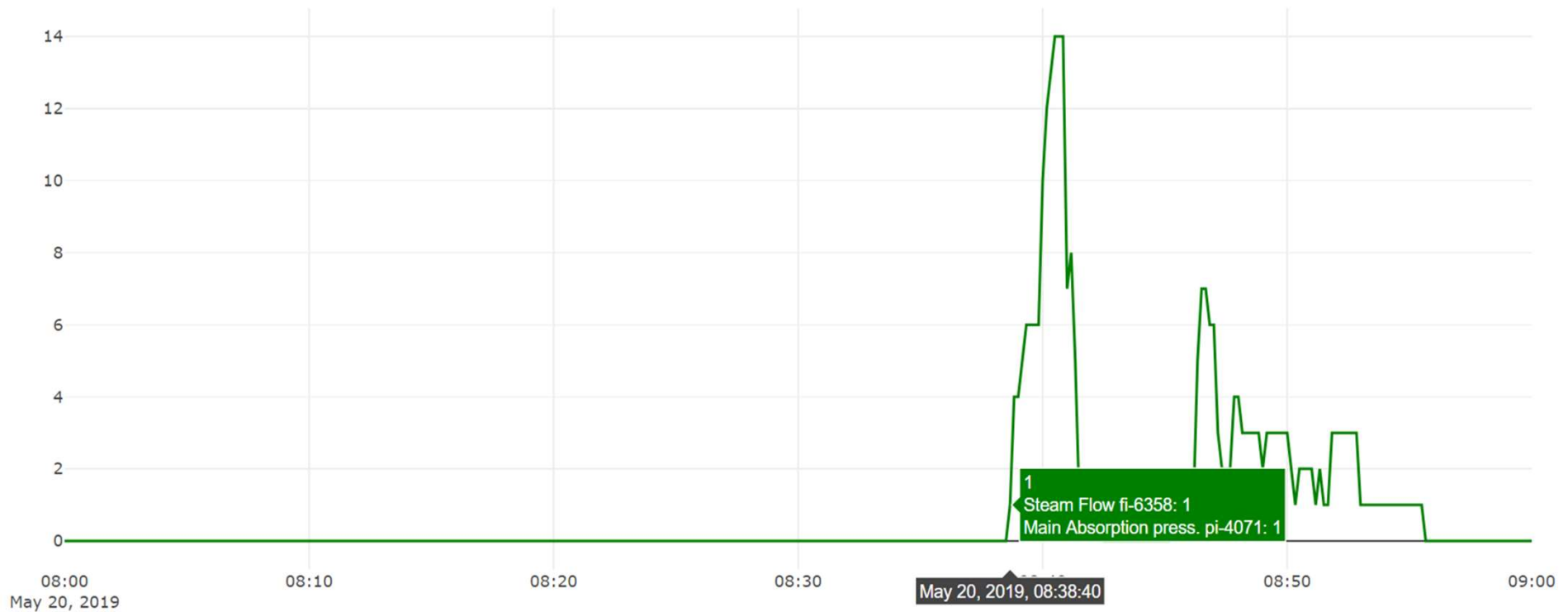*Elevating OT cybersecurity to Level 0*

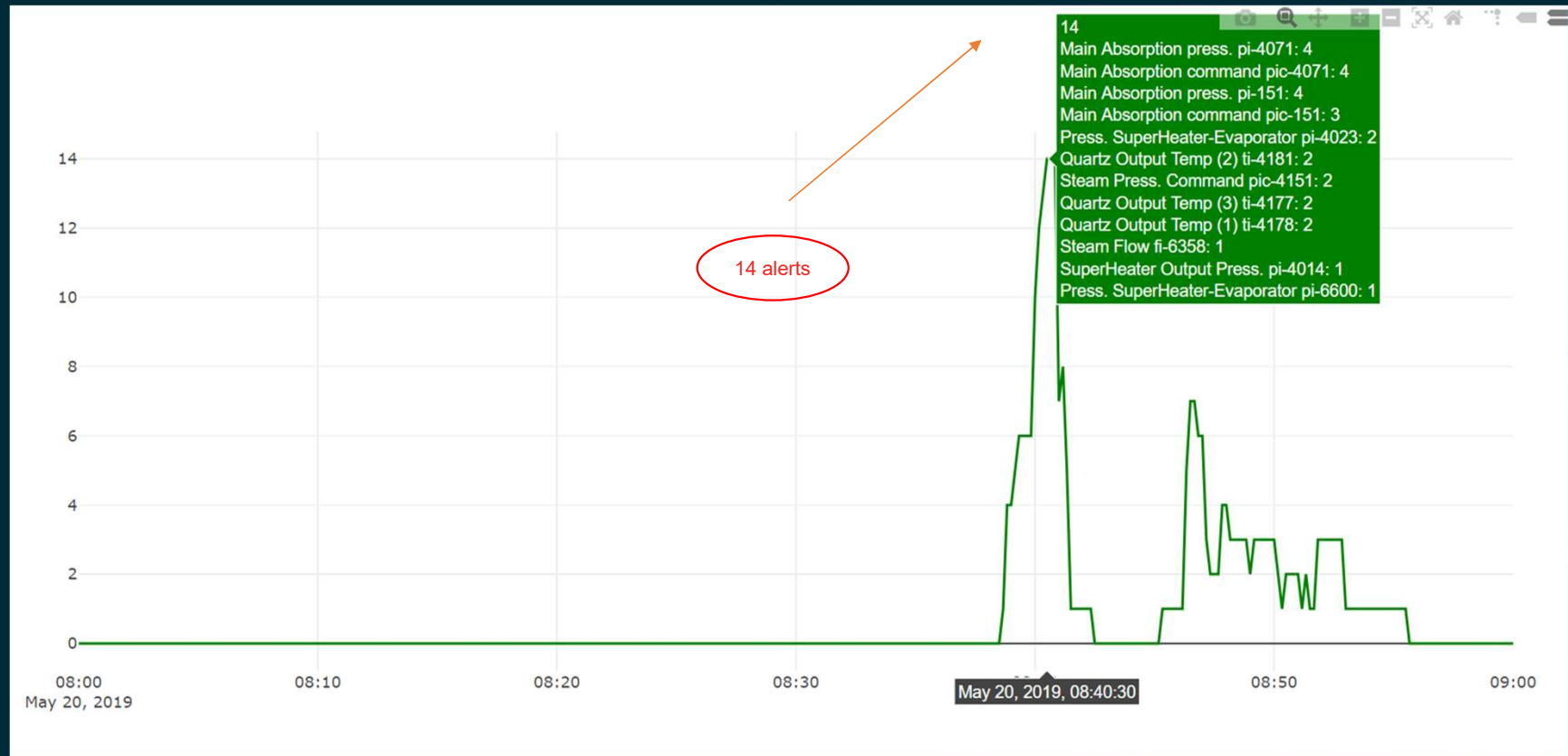# #1 – May 2019 – Steam + H Pressure drop

Switching of source steam supply to the line caused a change in <u>steam</u> and <u>hydrogen pressure</u>, which affected the <u>Bromine evaporator and superheater operation</u>, leading to a process shutdown at 08:44.
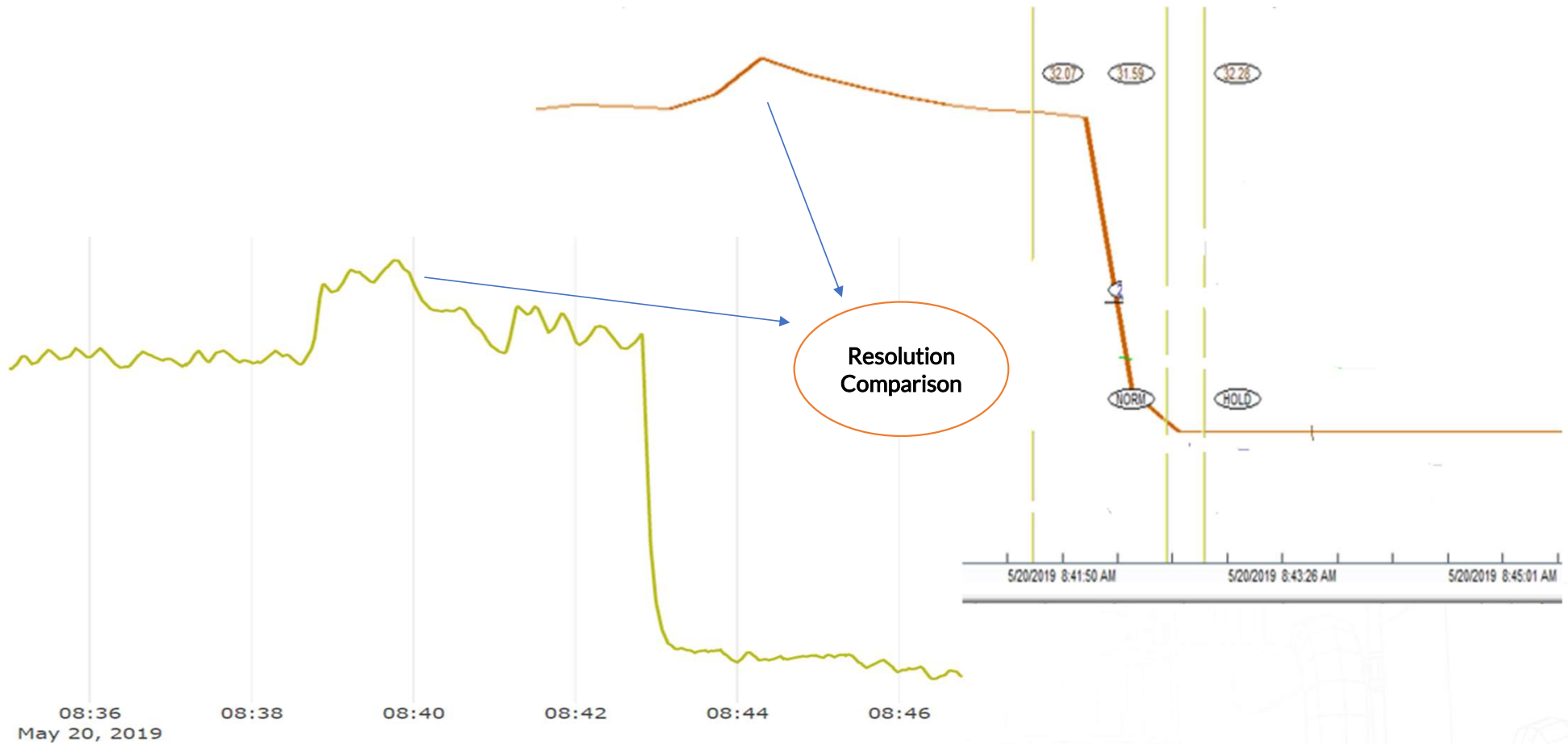

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0
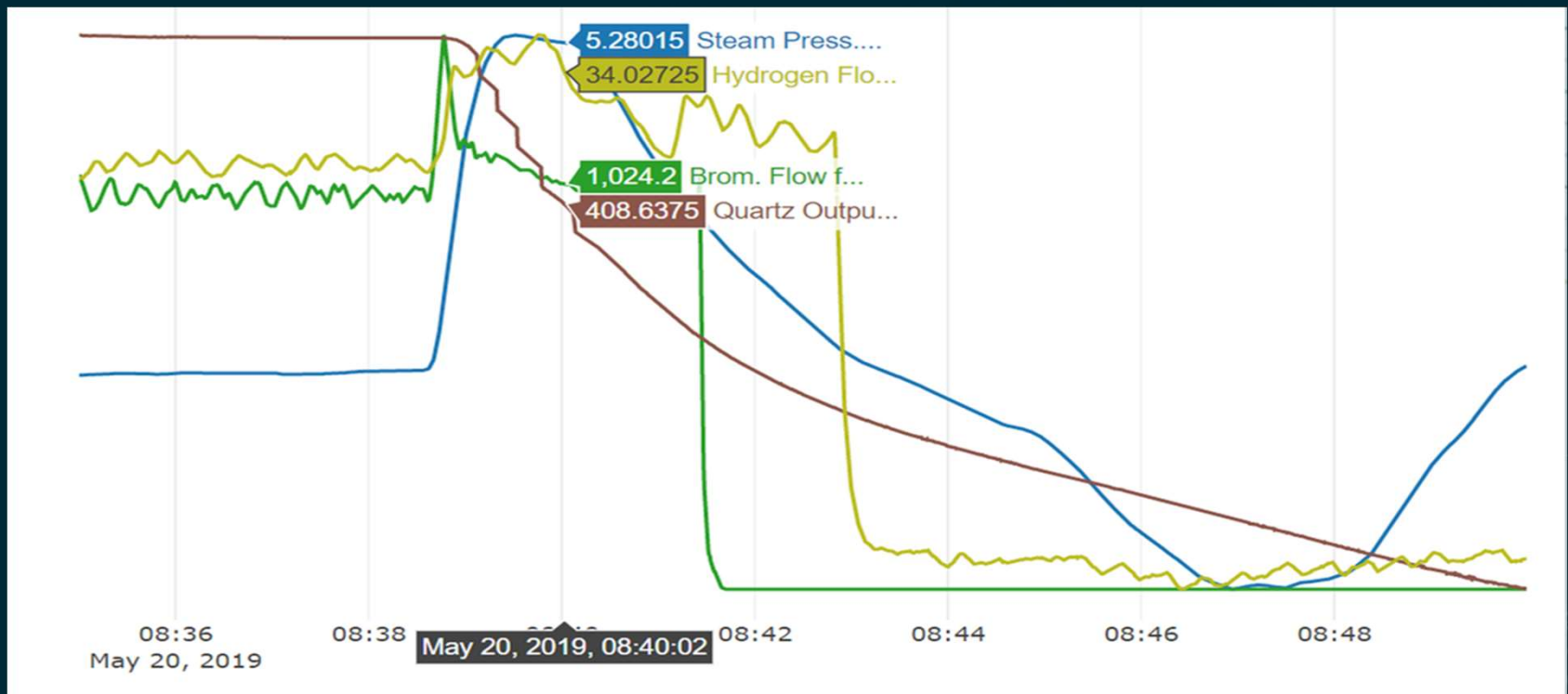
SIGA's Pre-Alert comes out <u>6 minutes</u> before production shutdown

SigaGuard reports 14 active alerts after 2 minutes

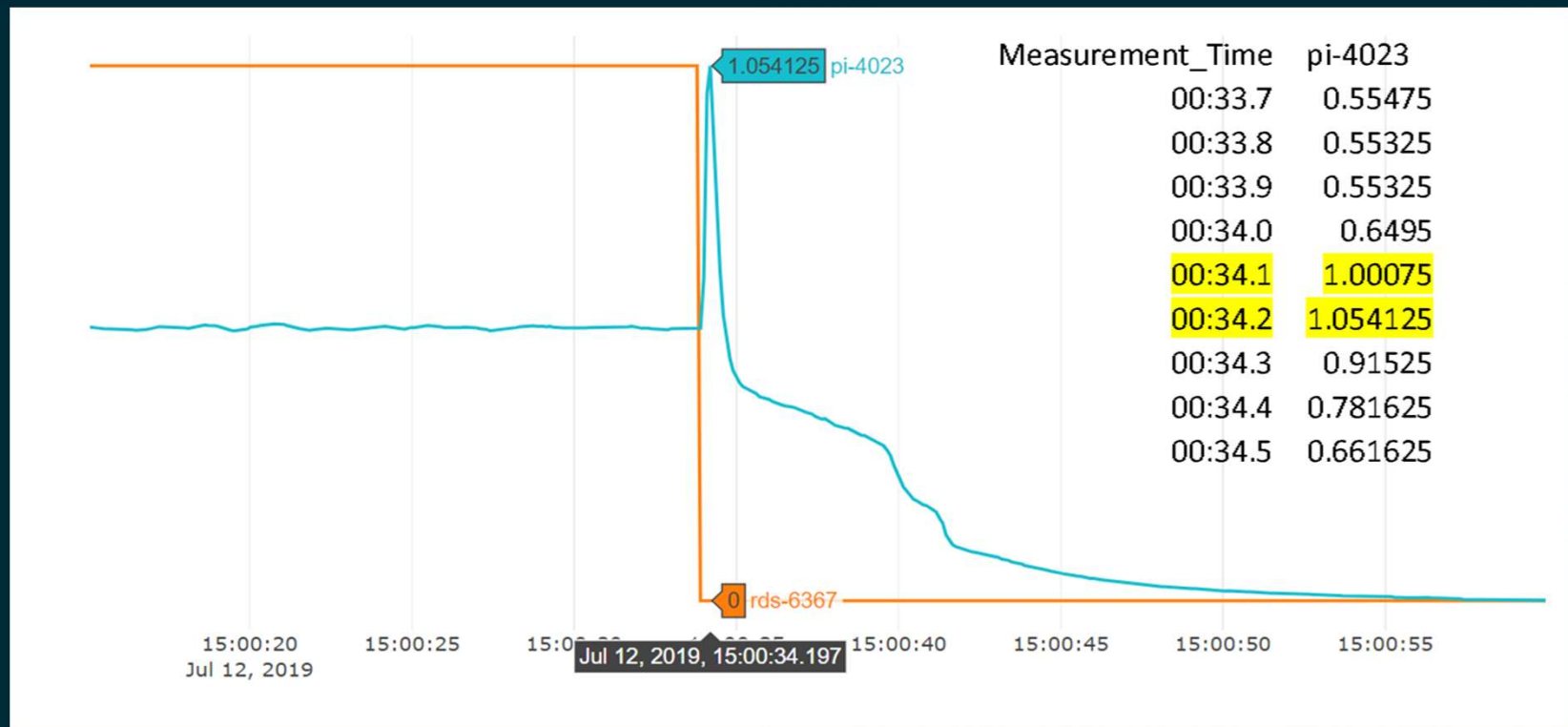14 alerts

14
Main Absorption press. pi-4071: 4
Main Absorption command pic-4071: 4
Main Absorption press. pi-151: 4
Main Absorption command pic-151: 3
Press. SuperHeater-Evaporator pi-4023: 2
Quartz Output Temp (2) ti-4181: 2
Steam Press. Command pic-4151: 2
Quartz Output Temp (3) ti-4177: 2
Quartz Output Temp (1) ti-4178: 2
Steam Flow fi-6358: 1
SuperHeater Output Press. pi-4014: 1
Press. SuperHeater-Evaporator pi-6600: 1

May 20, 2019, 08:40:30

May 20, 2019

Elevating OT cybersecurity to Level 0

SIGA
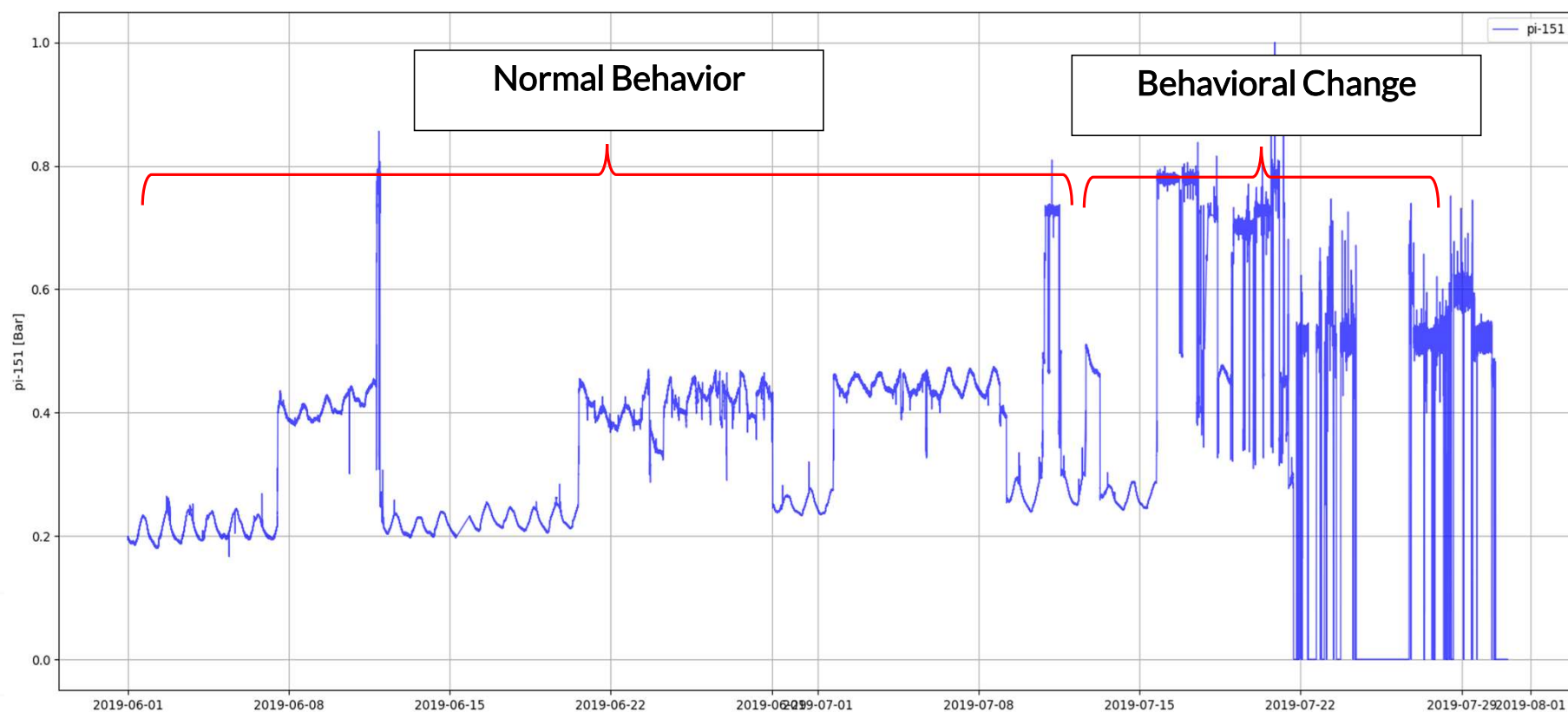Level Zero OT Resilience

Resolution Comparison Graphs

#2 – July 2019 – Discs Ruptures

With SIGA's system, plant engineers can obtain a high-resolution view for forensic analysis. Pressure bursts (PI >1bar) are only visible in SIGA's 10 measurements/sec resolution but are not visible in the HMI.

#3 – July 2019 – Sensor mis-calibration

Normal Behavior

Behavioral Change

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

#4 – January 2020 – Bromine flow malfunctions

About a minute before shutdown, SigaGuard issued a series of alerts (aggregations), focusing on bromine flow. A shutdown of Line 2 has been caused by undesired bromine flow (partial blockage in the pump) which has affected other parameters of the process causing abnormal behavior and eventually resulted in a shutdown..

Elevating OT cybersecurity to Level 0

SIGA
Level Zero OT Resilience
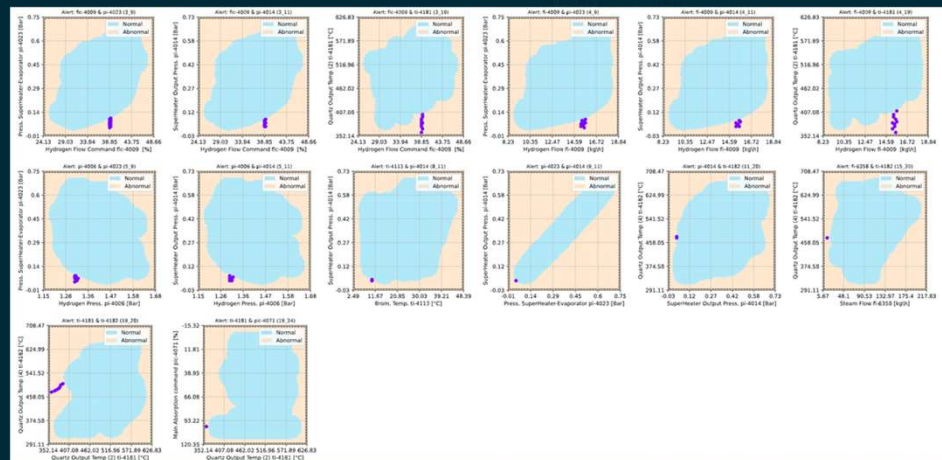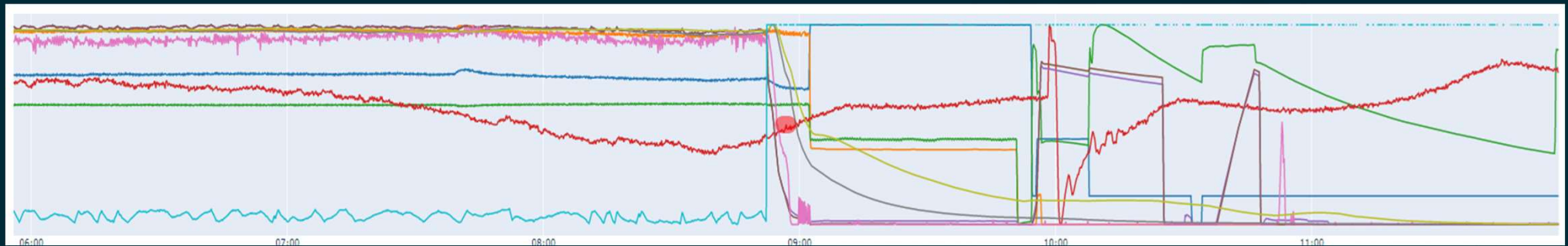
#5 – February 2020 – Hydrogen flow stoppage

The SigaGuard system issues a collection of alerts (aggregation) approximately one minute prior to shutdown. The message of the anomaly alert indicated that hydrogen pressure was the most influencing IO. AI features such as this are part of SigaGuard's clustering and explanation capabilities.

#6 – May 2020 – Bromine leakage

An anomaly in the Bromine pressure behavior was detected by SigaGuard and alerted the operator. As a result, the engineers examined the process in this area and discovered a Bromine leak in the quartz burner. This deviation is minor and does not cross any threshold, so the HMI was not notified.

Elevating OT cybersecurity to Level 0
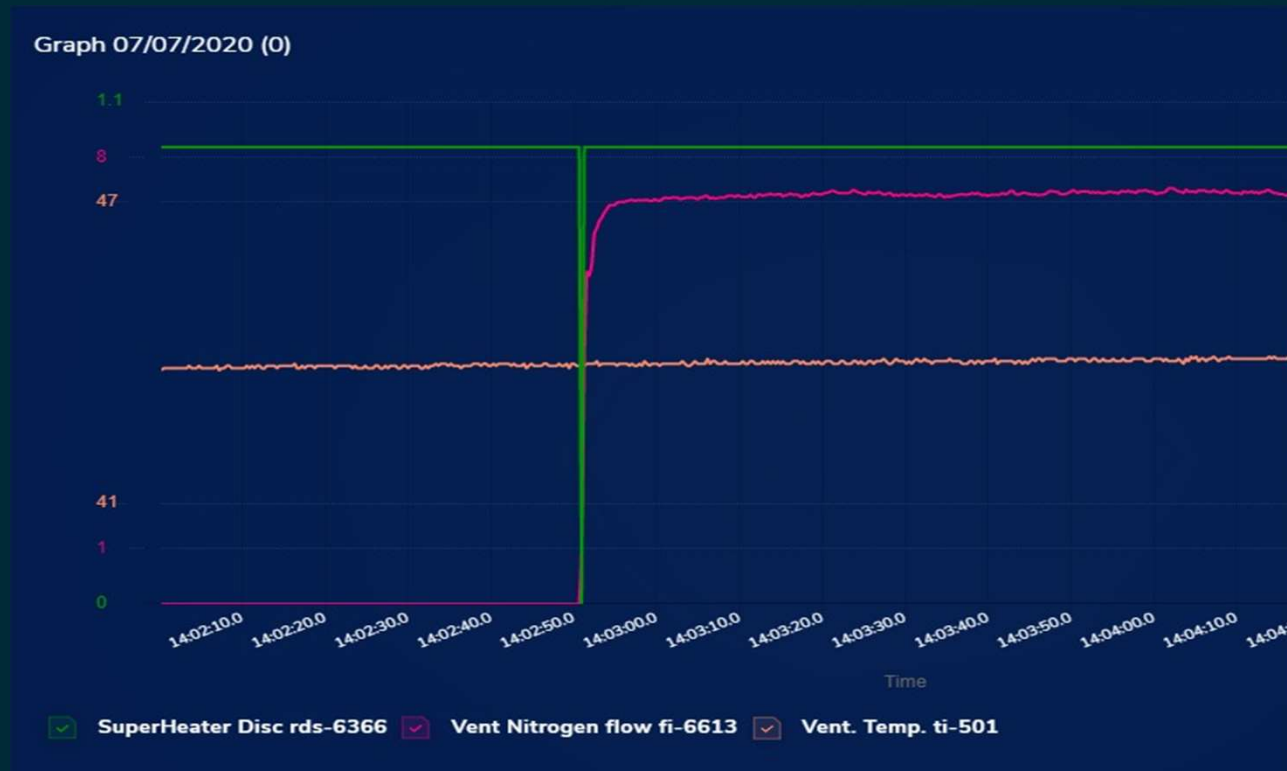
SIGA
Level Zero OT Resilience

#7 – June 2020 – Discs Rupture

SigaGuard detected and alerted on a disc rupture during the non-working hours of the engineers' team. The plant's engineers and facility engineers used SigaGuard system for forensics in order to understand the root-cause-analysis for this event to prevent future events.
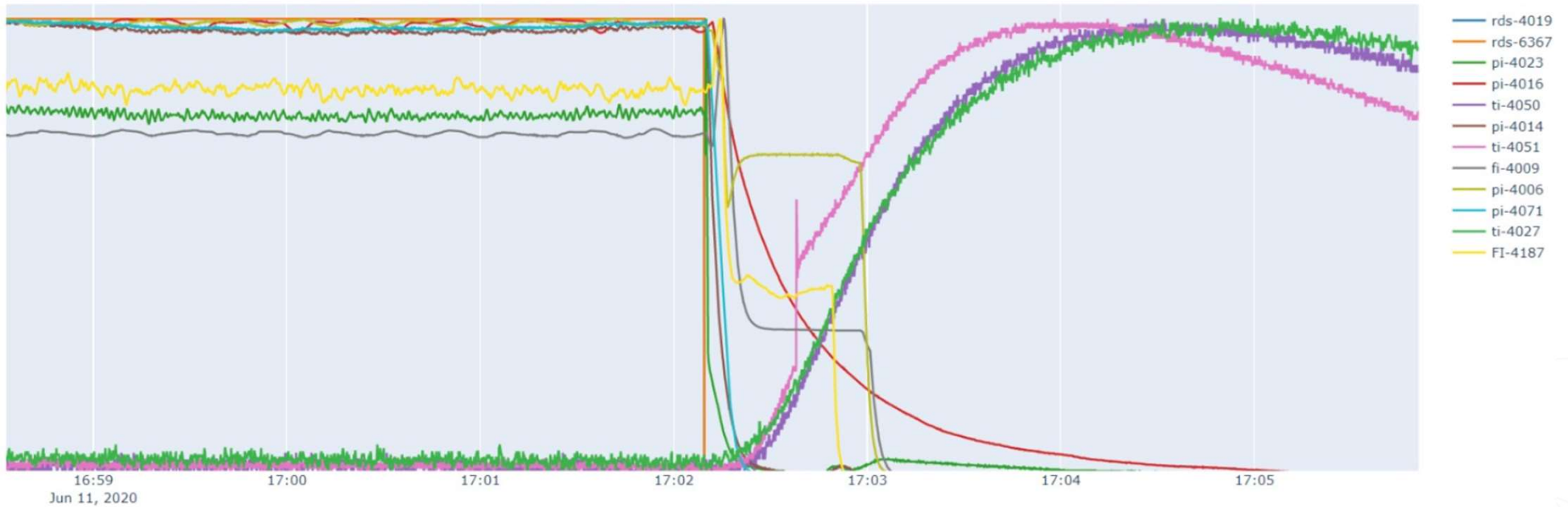
#8 – July 2020 – Disc malfunction

SigaGuard detected and alerted on a brief event of a disc rupture and a sudden ventilation flow change. 25 minutes later the process experienced a shutdown as a result of this abnormal behavior. After the engineer checked the machinery, they found a mechanical problem in the disc itself which they later fixed.

Graph 07/07/2020 (0)

Elevating OT cybersecurity to Level 0

SigaGuard unparalleled offering

The most advanced solution for detecting

and analyzing cyber-attacks on mission-

critical automated equipment, machinery

and processes.

Reduces downtime to a minimum: Unmatched visibility ensures a quick and safe recovery from downtimes.

Inaccessible insights: SigaGuard delivers precise granular visibility with cutting-edge AI insights.

Feeling the machinery's pulse: SigaGuard provides operators with the most reliable source of data

Data archives: Improved preparedness for future attacks

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

Conclusion

- Following the first successful year, the customer renewed his SigaGuard subscription in May 2020.

- The customer installed SigaGuard in this facility in 2019 and purchased three additional systems in 2020 for different sites. This customer is currently in the process of acquiring additional systems for additional locations through SIGA.

SIGA
Level Zero OT Resilience

Elevating OT cybersecurity to Level 0

About SIGA

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.

SIGA
Level Zero OT Resilience