AGGER
Powered by Gyala

INDUSTRIAL
CYBER RESILIENCE

IT/OT Cyber Resilience for the INDUSTRIAL sector

GYALA
Cyber Security

AGGER
Powered by Gyala

INDUSTRIAL CYBER RESILIENCE

5 Modules

Extended Detection and Response

Network Security Appliance

Risk Management Tool

Correlation Module

OT Defence

Gyala is the only Cyber Security vendor to have brought the automation of the Detection and Reaction Processes even within individual agents.

Agger is the only cyber security all-in-one platform **Made in Italy** that thanks to sophisticated AI algorithms developed for military use for supervision and automatic reaction, can prevent, identify, and automatically manage any IT threat and anomaly 24/7, maximizing infrastructure IT/OT resilience.

4 Features one platform

Detection

Identifies abnormal conditions by analyzing behavioural running processes in computers, traffic network, security logs already available in infrastructure and thanks to the integrity check and availability of OT devices.

Reaction

The reactions are performed by agents pre-configured with containment and mitigation actions that Cyber Security experts would perform by addressing various types of incidents or controlling actions on the system IT/OT itself, or guiding human operators with operating procedures detailed manuals. **The rules of reaction (and detection) are customizable for single agent/endpoint and OT system, to ensure the resilience of IT/OT services.**

Artificial Intelligence

It builds models of dynamic behavior - based on the data collected - then used to identify any deviations.

Investigation

It collects information, events and incidents useful for the post-analysis by the cybersecurity experts.

AGGER
Powered by Gyala

INDUSTRIAL CYBER RESILIENCE

CUSTOMIZABLE RULES ALSO FOR EACH AGENT

ALL-IN-ONE PLATFORM

CLOUD | ON PREMISE | SEGREGATED NETWORKS

SUPPORTS EVERY LEGACY SYSTEMS

IT/OT RESILIENCE

AUTOMATIC DETECTION & REACTION

EXTENSIVE THREAT INTELLIGENCE

PREVENTS | IDENTIFIES | MANAGES

AVERAGE REACTION TIME 0 SECONDS

AGGER TAILORED FOR EVERY MARKET:

How Agger works:

We install agents and probes or operate in **agentless mode**.

PASSIVE MODE:

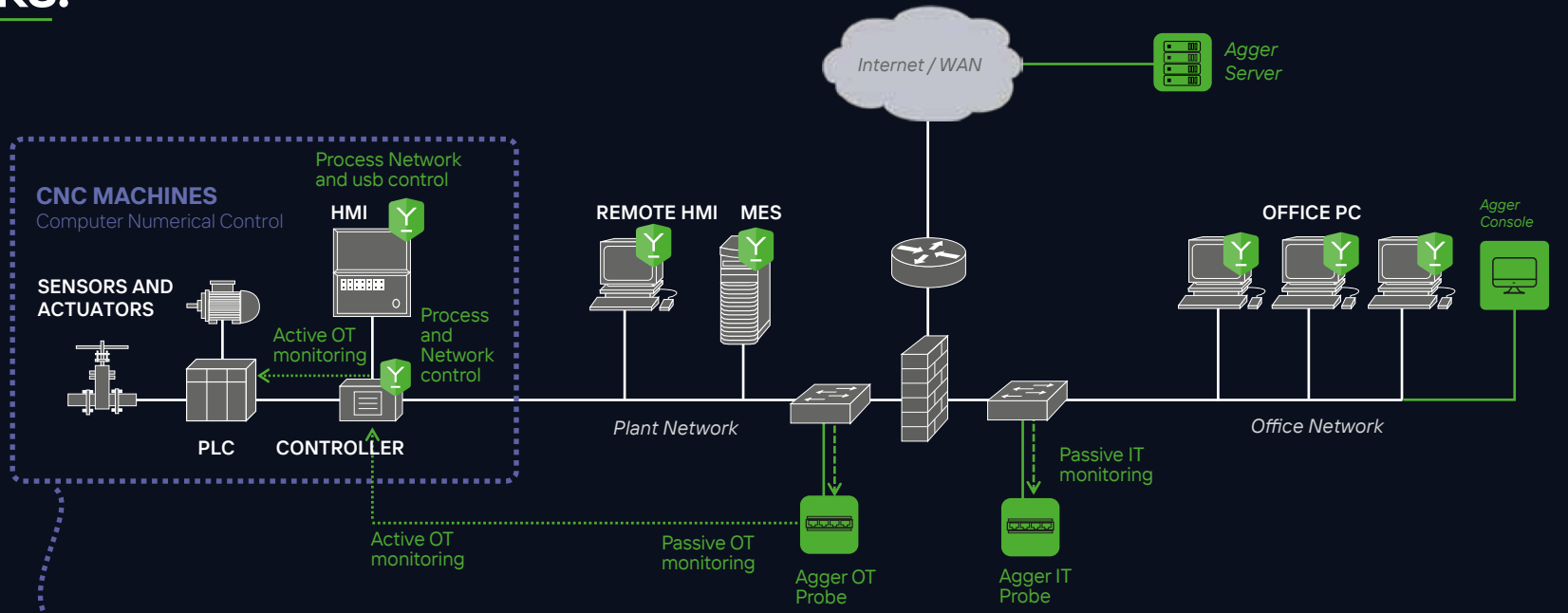
Based on network traffic duplication and interception, used to gather information about the behavior, performance, and security of an OT (Operational Technology) device or an entire OT system. It allows collecting and analyzing network communications of an operational system or device **without interfering with its normal operation.**

Agger Network Security is able to decode hundreds of standard OT protocols (S7, MMS, DNP3, OPC, MODBUS, PROFINET, ...) or to be extended with specific plugins for custom protocols.

ACTIVE MODE:

Monitoring achieved through direct interaction with the OT device, using the interfaces and protocols exposed by the device on the network. By acquiring much more information, it enables the detection of potential alterations to internal configurations made directly on the physical device.

Agger OT Defence actively interrogates networked OT devices, through periodic requests on standard protocols (S7, MMS, SNMP,...) and can be extended with specific plugins for custom protocols.



focus on the next page

note

- **Configuration of custom detection and reaction rules for both groups of agents and individual endpoints:** enables personalized incident management based on the operational role of impacted assets. The set of possible reactions is extremely broad. Complex sequences of actions can be created to be executed in real-time on the machine that generated the incident, on those belonging to the same potentially at-risk service, or on the entire IT or OT infrastructure.
- Collection of information about the system's state at the moment an incident occurs, made available to the analyst along with the applied rules to contain it. It allows verifying the system's state at the time of the incident: running processes, network connections, logged-in users, routing tables, service status, changes to task manager configurations, users and groups, network configurations, installed software, etc.
- Ability to assign tags (color and text) to endpoints and agentless devices to attribute information such as the physical location of the device, the service to which it belongs, the provider managing it, etc.

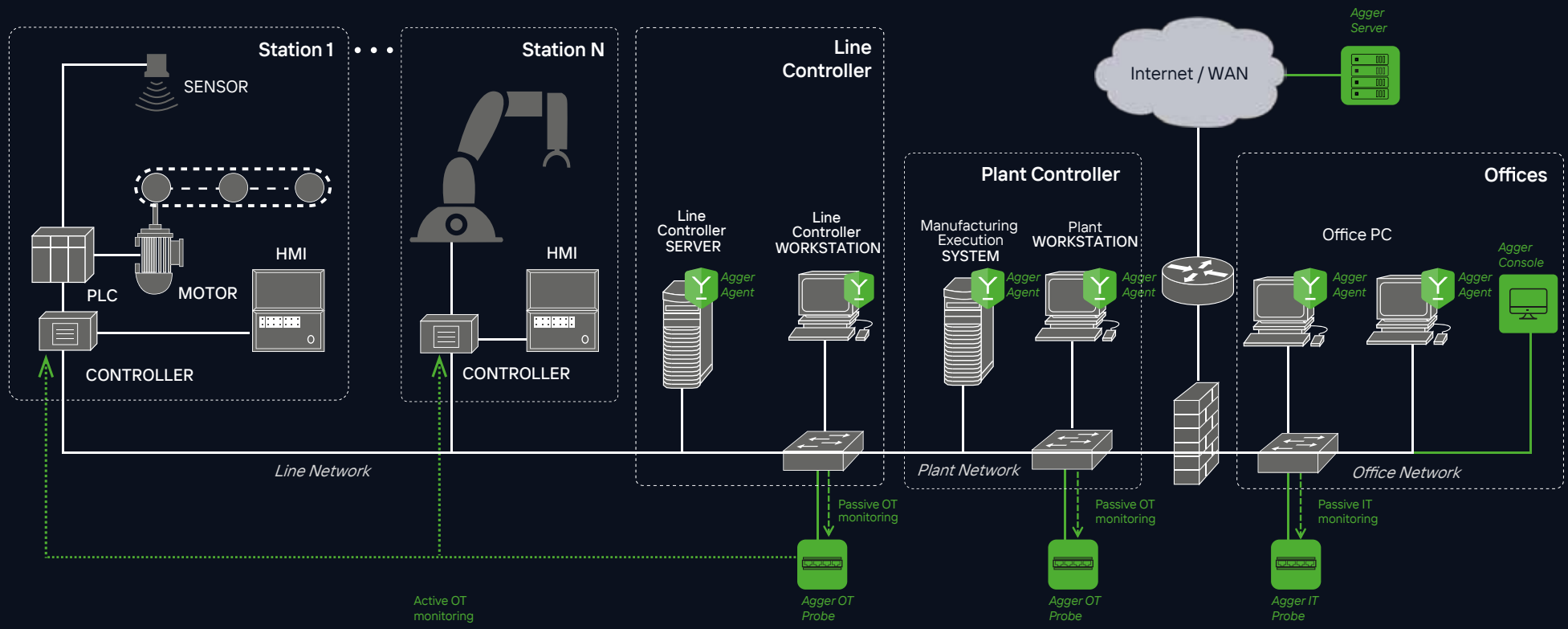
PRODUCTION LINES

The increasing convergence between IT and OT has brought significant operational and economic advantages but has inevitably expanded the vulnerability perimeter of infrastructures and businesses by interconnecting two historically and culturally separate worlds.

The increased frequency of attacks on critical infrastructures and industrial sites **has highlighted the structural weaknesses of the OT world**, which, not having been exposed to such threats before, has not adopted secure-by-design approaches.

To ensure the continuity and integrity of production processes, increasing resilience against cyber threats is crucial. **It is essential to adopt a holistic approach that integrates technological and procedural aspects.**

Gyala has developed a process to secure industrial plants through solutions dedicated to various types of machines and production lines, ensuring full compliance with the requirements of the European Machinery Safety Regulation and the National Cybersecurity Framework.

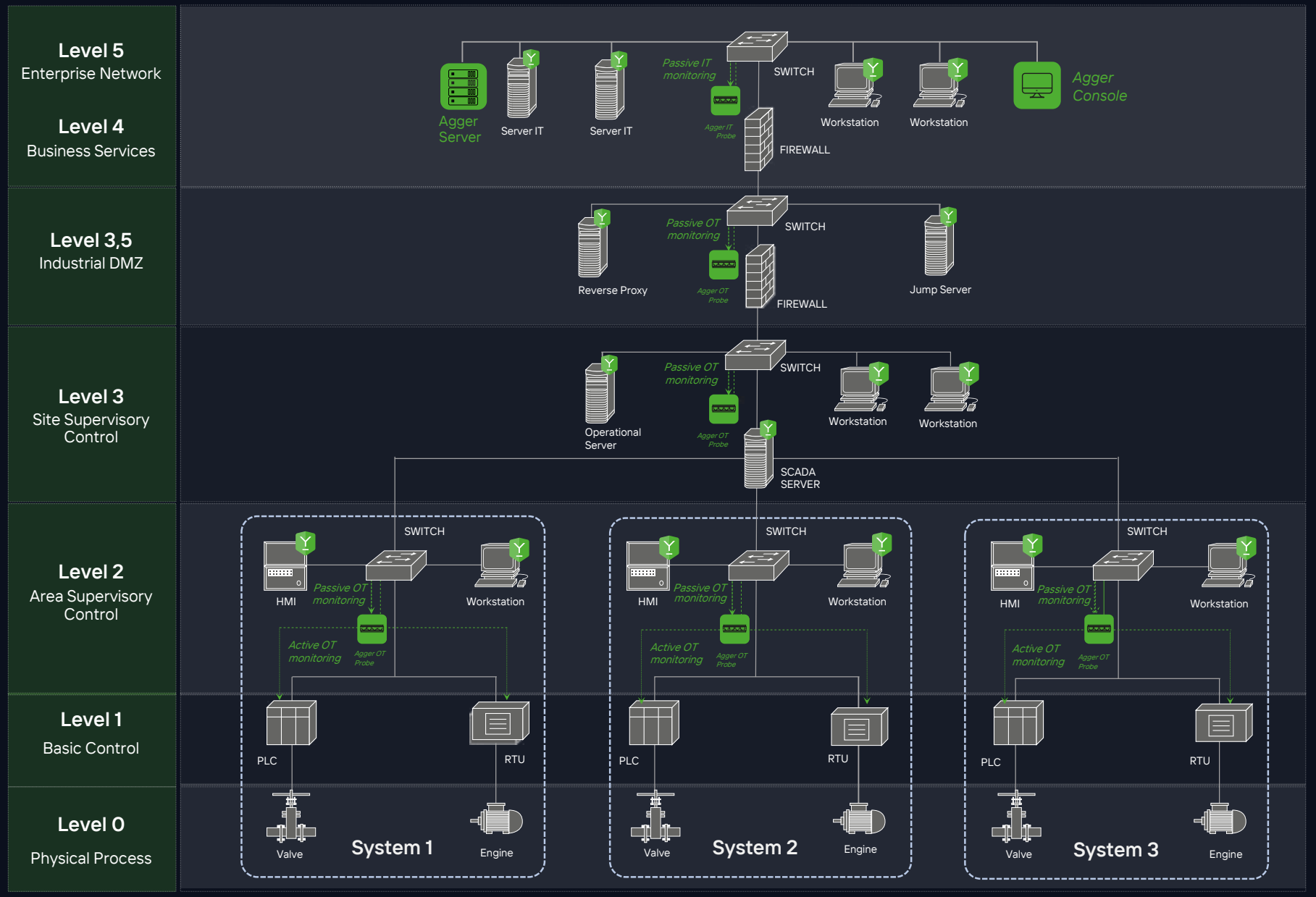


PURDUE MODEL

Purdue Enterprise Reference Architecture

IT
We perform passive monitoring of IT traffic. We install agents on clients and servers and actively query network devices.

OT
We do passive traffic analysis and active interrogation of OT devices. We install agents on control computers and HMIs.



Gyala,
Safe. **Always.**

Agger, Custom Made Solution

Agger, our **Cyber Security all-in-one** totally modular and customizable according to needs, thanks to sophisticated AI algorithms developed for military use for supervision and automatic reaction, can prevent, identify, and automatically manage any IT threat and anomaly 24/7 and guarantee the IT/OT resilience.

Agile approach to innovation

Gyala combines **the "agile" approach** typical of an innovative start-up with the consolidated **know-how gained** by the three Founders in the management of Cyber Protection projects for critical infrastructures, developed with various Ministry of Defence units and major national System Integrators.

We develop advanced autonomous cyber defense systems to protect companies' strategic IT and OT public and private assets from cyber attacks.

Gyala, your Technology Partner

Thanks to our **many years of experience in the Defense Sector,** we deal with competence and **with maximum efficiency** the growing challenges of the cybersecurity landscape.

We use an ecosystem of system integrators, consulting firms and solution providers that integrate our solution within the customer's infrastructure.

ISO 9001:2015
ISO IEC 27001

INDUSTRY 4.0

CYBERSECURITY MADE IN EUROPE

marketing@gyala.com
gyala.com in Gyala