AGGER

Powered by Gyala

NAVAL
CYBER RESILIENCE

IT/OT Cyber Resilience for the NAVAL sector

GYALA
Cyber Security

AGGER

Powered by Gyala

NAVAL 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 conditions abnormal 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.

Artificial Intelligence

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

Reaction

The reactions are performed by agents previously instructed with the actions of containment and contrast 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, allowing you to get the resilience of IT/OT services defended.**

Investigation

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

AGGER

Powered by Gyala

NAVAL
CYBER RESILIENCE

CUSTOMIZABLE RULES
ALSO FOR EACH AGENT

ALL-IN-ONE PLATFORM

CLOUD | ON PREMISE | SEGREGATED NETWORKS

SUPPORTS EVERY LEGACY SISTEMS

IT/OT RESILIENCE

AUTOMATIC DETECTION & REACTION

EXTENSIVE THREAT INTELLIGENCE

PREVENTS | IDENTIFIES | MANAGES

AVERAGE REACTION TIME
0 SECONDS

AN AGGER FOR EVERY MARKET:

INDUSTRIAL
CYBER RESILIENCE

NAVAL
CYBER RESILIENCE

HEALTH
CYBER RESILIENCE

ENTERPRISE
CYBER RESILIENCE

PMI
CYBER RESILIENCE

UTILITIES
CYBER RESILIENCE

PA
CYBER RESILIENCE

DEFENCE
CYBER RESILIENCE

FINANCE
CYBER RESILIENCE

How Agger works:

We install agents and probes or operate in **agentless mode**.
In fact we overcome the problem of impossibility of installing software agents on the programmable logic of OT devices thanks to a sophisticated device interrogation te chnique implemented in agentless mode.

PASSIVE MODE:

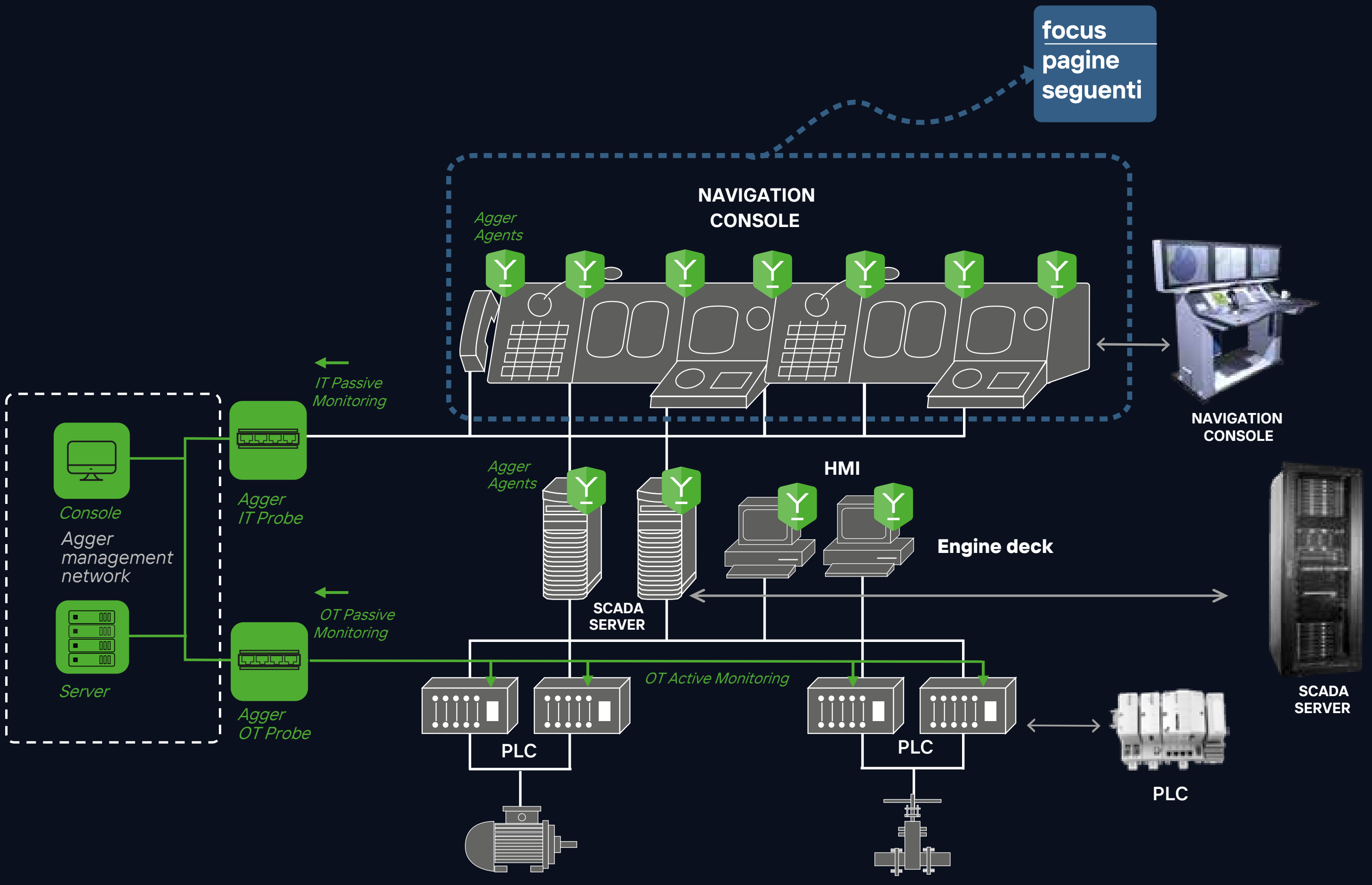
Based on network traffic duplication and interception, used to gather information about the behavior, performance, and security of an OT (Operational Technology) device or an entire OT system. It allows collecting and analyzing network communications of an operational system or device **without interfering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



Since July 1
2024
Mandatory

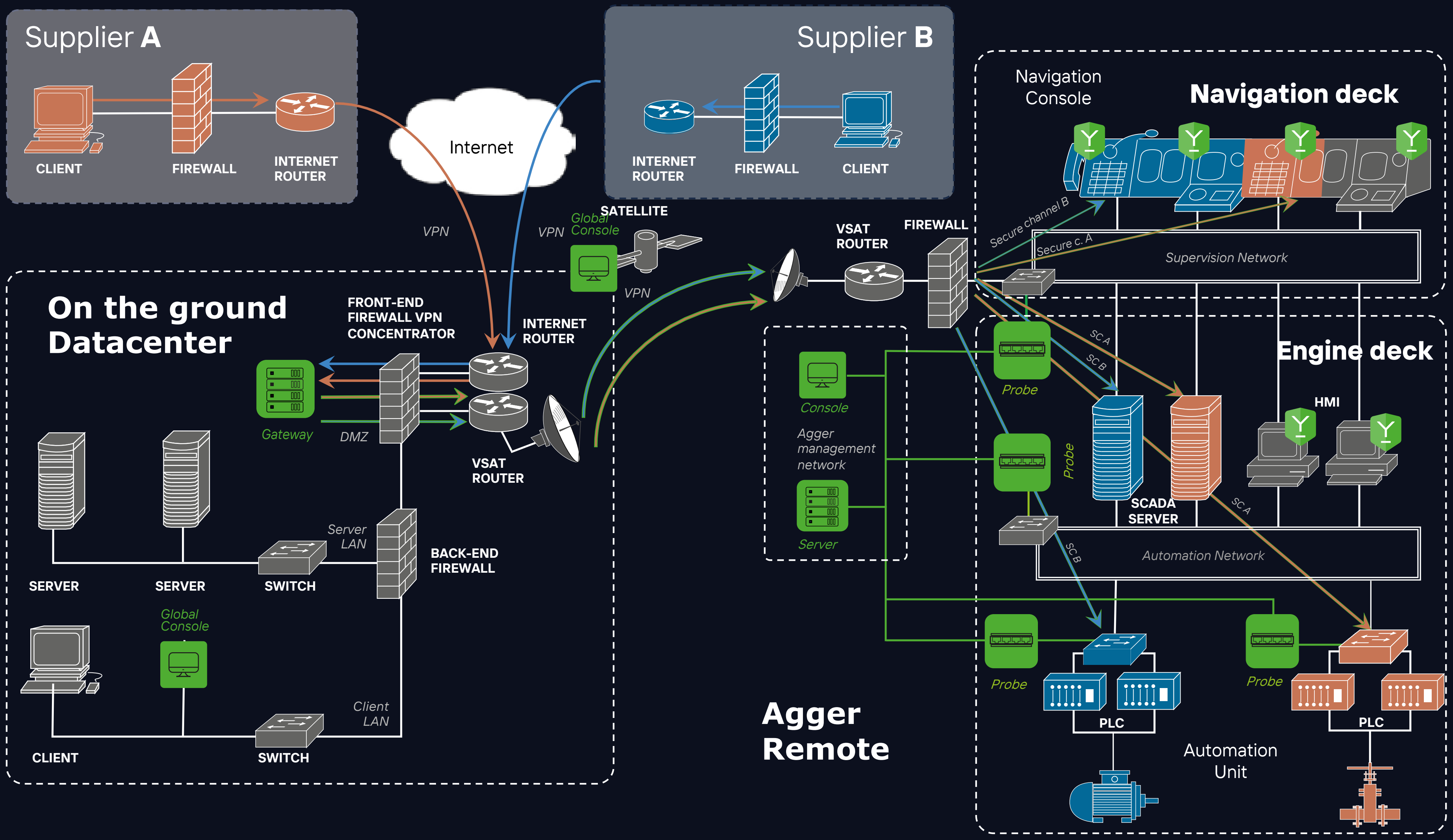
Ensures the compliance with the standards thanks to Agger Naval Resilience

Standard IACS

International Association of Classification Societies

The UR-E26 "Cyber resilience of ships – Rev.1 Nov 20232" e UR-E27 "Cyber resilience of on-board systems and equipment – Rev.1 Sep 2023" standards **are mandatory for the ships that they will be ordered since 1st July 2024, and are suggested as guidelines for previous.**

The first standard provides the requirements for the cyber security of the ship as a whole, while the second for the individual subsystems.



SHIP MANAGEMENT SYSTEM

Objective: The resilience of a ship's IT/OT infrastructure by providing secure and controlled access for remote diagnostics and maintenance service providers.

Agger provides a ground-based Secure Gateway that verifies supplier access and enables secure and segregated communication channels through satellite services to each ship. The Control Center Console allows you to define simple policies that allow a supplier to access only predefined subsystem equipment on a specific ship in a predetermined time window. The Secure Gateway logs all supplier sessions and checks in real time that no operations are performed that violate security policies.

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 garantee 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 cutting-edge Automatic Defense solutions 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, advisor company and solution providers that integrate our solution within the customer's infrastructure.

ISO 9001:2015
ISO IEC 27001

COMPLIANT
WITH THE
IACS STANDARDS
UR-E26 e UR-E27

CYBERSECURITY
MADE IN EUROPE

more info: marketing@gyala.com - www.gyala.com

GYALA
Cyber Security

marketing@gyala.com
gyala.com in Gyala