

OT Connectivity & Cybersecurity ●  
Open Architecture Edge Computing ●  
VoIP Security ●

# NAONWORKS

 KOREA

 Ministry of SMEs and Startups |  KBIZ Korea Federation of SMEs

 أديبيك  
ADIPEC |  ادينوك  
ADNOC Host

31 October - 3 November 2022  
Abu Dhabi, United Arab Emirates



**NAONWORKS**  
an AhnLab Company

# NAONWORKS

an AhnLab Company

With over 10 years of R&D and customer experience, NAONWORKS has led the convergence security market in Korea.

As IT and OT converge, there comes the need for secure and streamlined digital transformation(DX). For Smart Factory, Smart City, Smart Oil&Gas and Smart Office, we offer connectivity and security solutions based on industrial protocol inspection and open architecture-based edge computing.



*BEYOND SMART, Security is the last piece in your DX puzzle!*

## Certifications

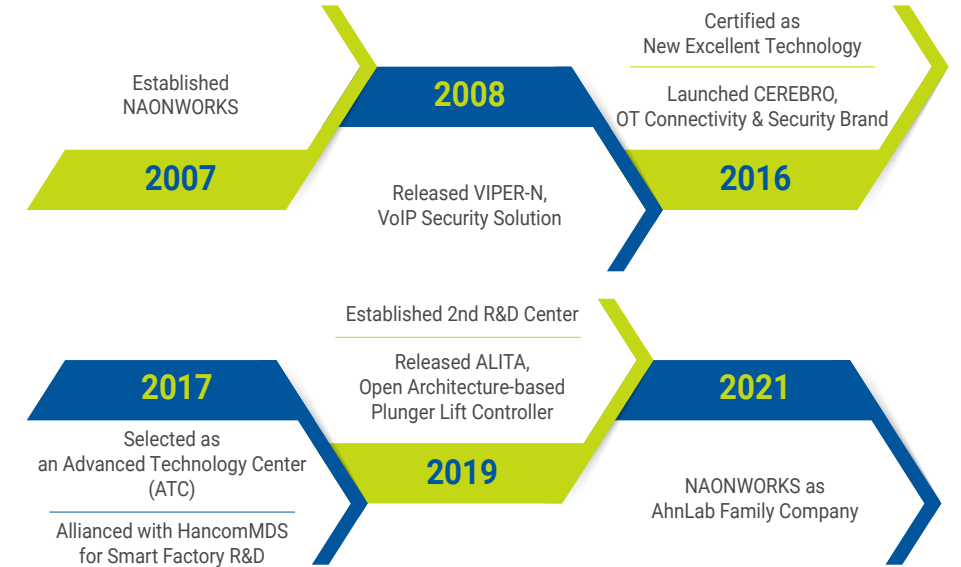


## Patents

VoIP Security  7+

OT Security  6+

## History



## Business Areas & Solutions



### OT Connectivity & Security *CEREBRO*

CEREBRO-C | Industrial Protocol Gateway For Plant Floor Communication

CEREBRO-DD | Unidirectional Security Gateway Solution

CEREBRO-DP | Industrial Protocols DPI(Dep Packet Inspection) Solution



### Edge Computing Platform *ALITA*

ALITA | Open Architecture Plunger Lift Automation Solution



### VoIP Security *VIPER*

VIPER-N | VoIP Security Gateway Solution



## Contents

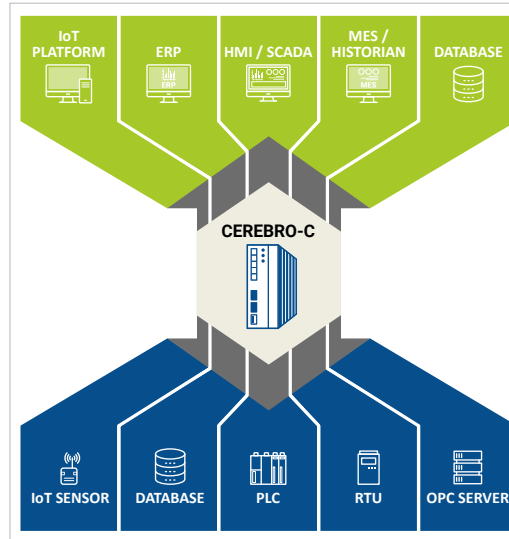
- 01 CEREBRO-C
- 02 CEREBRO-DD
- 03 CEREBRO-DP
- 04 ALITA
- 05 VIPER-N

# CEREBRO-C

## Industrial Protocol Gateway For Plant Floor Communication

CEREBRO-C is a connectivity solution for the real-time data access and seamless device communication in plant floor.

When establishing a system for site integrated management or implementing a new facility, you can resolve the linkage challenges due to various and different communication protocols. All you need is CEREBRO-C, and there is no need to change the existing network configuration.



- Hundreds of devices data collection**
- Simultaneous & direct connections to clients** such as HMI/SCADA, MES, IoT platforms
- Secure communication environment** encrypted communication between devices
- Customized solution** without limitation on hardware and platform

### Application Areas



### Features

<b>Protocol Standardization</b>	<ul style="list-style-type: none"> <li>Converts various industrial protocols into standards</li> <li>Secures communication and endpoints with OPC-UA standardization</li> </ul>
<b>OPC Interoperability</b>	<ul style="list-style-type: none"> <li>Provides OPC-UA/DA server service</li> <li>Provides OPC-UA/DA client/serial/Ethernet interface drivers</li> </ul>
<b>Streamlined Digital Transformation</b>	<ul style="list-style-type: none"> <li>Supports linkage based on the higher system interface such as SCADA, MES/ERP, etc.</li> <li>Removes dependency on manufacturer/version/protocol when introducing new equipment</li> </ul>
<b>Supported Protocols</b>	<ul style="list-style-type: none"> <li>Supports the connectivity between hundreds of industrial devices</li> <li>Includes non-standard protocols such as domestic PLC</li> </ul>
<b>Customer Optimization</b>	<ul style="list-style-type: none"> <li>Supports multi-platforms such as Windows, Linux, and Container(Docker)</li> <li>Provides hardware options for an ultra-small device/embedded-type/existing equipment, etc.</li> <li>Supports interfaces exclusively for special and non-standard devices such as IoT</li> </ul>

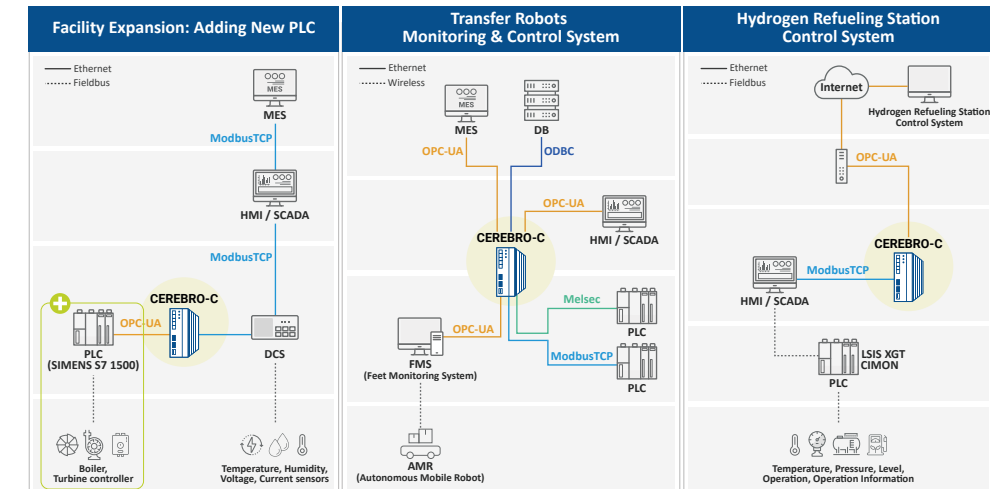
### Major Functions

Service	Management
<ul style="list-style-type: none"> <li><b>* Protocol Gateway</b> <ul style="list-style-type: none"> <li>Standardizes and converts various industrial protocols</li> </ul> </li> <li><b>* OPC-UA Server/Client</b> <ul style="list-style-type: none"> <li>Links OPC-UA standard protocol, update buffering function</li> </ul> </li> <li><b>* OPC-DA(Classic) Server/Client</b> <ul style="list-style-type: none"> <li>Windows-based OPC-DA(Classic) Server</li> </ul> </li> <li><b>* Communication Security</b> <ul style="list-style-type: none"> <li>Encrypted, authenticated, and secure communications from client to device across network topologies</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>* Device Tag Management</b> <ul style="list-style-type: none"> <li>Provides simultaneous device data in the unit of tag</li> </ul> </li> <li><b>* Device Communication</b> <ul style="list-style-type: none"> <li>Functions to read/write device data</li> <li>Device communications status management</li> </ul> </li> </ul>
<b>Customization</b>	
<ul style="list-style-type: none"> <li><b>* Additional support for specific driver/service protocols</b></li> <li><b>* Interface support for special/non-standard devices</b></li> </ul>	

### Supported Protocols

Driver		Service	
Modbus ASCII/RTU	Ping	SIEMENS	S7 Ethernet
Modbus TCP	SNMP	Mitsubishi	Mitsubishi Serial/Ethernet
OPC-UA Client	WebSocket	Mitsubishi	Mitsubishi CNC Ethernet
OPC-DA Client		CIMON	CIMON Serial/Ethernet
DN3 Serial/Ethernet		AB	Ethernet/IP
DeviceNet		OMRON	CS/CJ Ethernet
EtherCAT Master		Yokogawa	FAM3 Serial/Ethernet
EthernetIP Scanner		Yaskawa	Memobus Ethernet
HART		Fuji	Micrex-SX Ethernet
BACnet/IP		KEYENCE	Keyence Serial/Ethernet
LS Electric	Master-K	FATEK	Fatek Serial/Ethernet
	GLOFA-GM Serial/Ethernet	FANUC	FANUC Ethernet
	XGT Serial/Ethernet	AutomationDirect	AutomationDirect Serial

### Use Cases



# CEREBRO-DD

## Unidirectional Security Gateway Solution



### Physical Unidirectional

Hardware-based network separation  
No return path to data sources

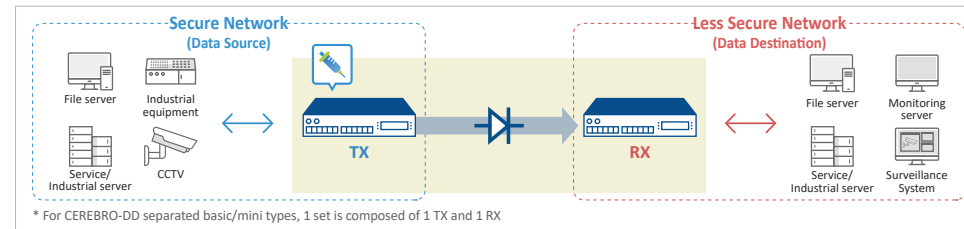
### Zero-Risk Communication

Non-routable unidirectional protocol  
Forward Error Correction for no packet loss

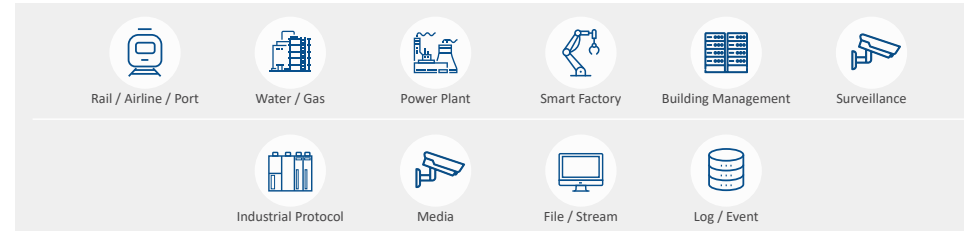
### Enhanced Security

NIS verified encryption module  
Vaccine for malware scanning

**CEREBRO-DD** protects data sources such as OT networks and enables secure data transfer from data sources to destinations in less secure networks. Because there is no return path to the data source, sensitive assets in the source network are isolated from external security threats. To enhance security, CEREBRO-DD uses non-routable protocol in the unidirectional communication section, and only transfers safe data after policy inspection, signature inspection, and malicious code inspection. It ensures the reliability of transmission with forward error correction(FEC).



### Application Areas & Services



### Features

<b>Security</b>	<ul style="list-style-type: none"> <li>Complies with functional requirements for unidirectional security gateway/data diode</li> <li>Encryption of transferred data between components</li> <li>Administrator policy/signature/malware inspections before data transfer</li> </ul>
<b>Reliability</b>	<ul style="list-style-type: none"> <li>Encryption module verified by the National Intelligence Service(NIS)</li> <li>Transmission reliability with Forward Error Correction(FEC)</li> <li>Guaranteed throughput up to 10 Gbps</li> </ul>
<b>Scalability</b>	<ul style="list-style-type: none"> <li>Same hardware scales from 1 to 10 Gbps for the unidirectional transfer section</li> <li>Highly available environment in a redundant configuration</li> <li>Power source Single AC or Redundant AC</li> </ul>
<b>Flexibility</b>	<ul style="list-style-type: none"> <li>Various communication support including Industrial protocols, media, files, DB.</li> <li>Provided as an appliance to the exclusive hardware</li> <li>Supports specific linkage programs compatibility and customization</li> </ul>

### Major Functions

#### Service

##### \* Zero-Risk One-way Communication

- Transmission server(TX) and receiving server(RX) are physically separated (detached type)
- Only the TX line is connected physically, while the RX line is disconnected
- No reverse transmission from less secure networks to secure networks
- Real-time data transmission without data loss

##### \* Redundant Configuration Option

- Redundant configurations of transmission and receiving servers for stability
- Performs the failover when equipment or line fails

#### Security

##### \* Data Integrity

- A log is generated when there is data loss
- Transmission management functions; error recovery codes, and transmission rate control
- Management functions; error test and recovery in receiving process, packet loss and receiving failure management

##### \* Secure Data Communication

- Data control setting when network ports of the transmission server and receiving server are disconnected
- Safe and exclusive unidirectional protocol, not TCP/IP

##### \* Encryption

- Guaranteed confidentiality and integrity through the encryption of data transmitted between equipment

##### \* Malware Scanning

- Option 1: AhnLab TS Engine based Inspection
- Option 2: Multi-engine vaccine based Inspection

#### Management

##### \* Log Management

- Data transmission logs and system audit logs
- Log records are saved for over 365 days

##### \* Access Management

- Real-time access status and access history
- Blocks access and locks user account when the administrator's authentication fails

##### \* Setting Management

- Based on the guideline of analyzing and evaluating the vulnerability of information & communication infrastructure
- Real-time policy setting for the administrator

### Supported Protocols

<b>Media</b>	(S)RTP, RTCP, RTSP	<b>Industrial Protocol</b>	OPC UA/DA/AE, Modbus
<b>File</b>	(S)FTP, File, Folder, HTTPS	<b>IT Protocol</b>	Emerson, MelsecA/Q, SIEMENS S7, GLOFA-GM, Fatek, LSIS XGK/XGI/XGB/XGR, MASTER-K, DNP3, CIMON, Unitronics, Omron, BACnet, Yaskawa, Yokogawa, etc.
<b>DB</b>	MS_SQL, Oracle, MySQL, DB2, Tiberio, etc.	<b>IT Protocol</b>	Syslog, UDP, TCP, SNMP

### Product Types

Based on minimum specification

Type	Separated Basic	Integrated Basic	Separated Mini
CPU	Intel Quad-core 3.6GHz	Intel Quad-core 1.6GHz	Intel Dual-core 2.2GHz
Memory	16GB	8GB	8GB
HDD	1TB	250GB	120GB
NIC	10/100/1000Mbps 8ports	10/100/1000Mbps 2ports	10/100/1000Mbps 2ports
One-way NIC	1~10Gbps Fiber X 2ports	1Gbps Fiber X 1port	100Mbps X 1port

\* Hardware specifications for each product may change according to the customer environment.  
\* The server may change due to the manufacturer's circumstances.

# CEREBRO-DP

## Industrial Protocol DPI Probe

\*DPI (Deep Packet Inspection)

### MONITOR

Real time data collection in mirroring mode



### INSPECT

Deep inspection on OT control data



### CONNECT

OT protocols conversion to IT protocols

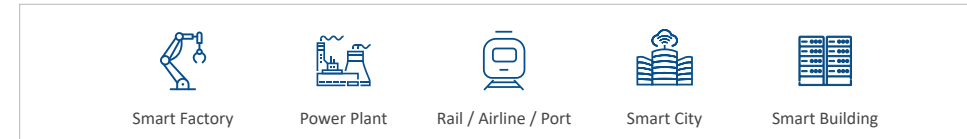


The key to industrial site security is real-time integrated management and control system for the entire network.

**CEREBRO-DP** is a DPI probe solution for industrial control data that provides the broadest insights into OT networks. Based on expertise in various communication protocols within factory automation systems, CEREBRO-DP monitors and in-depth analyzes all network and control data in real-time. In addition, it interlocks with the upper IT system to determine whether the control data is abnormal and immediately reports security issues to enable safer and loss-free operation of industrial sites.

CEREBRO-DP provides functions to identify, analyze, and convert protocols in various OT and IT domains through proprietary protocol profiling technology and analysis functions. In addition, it is a security solution that allows you to manage the system reliably without worrying about downtime by using a passive monitoring method that does not interfere with the existing process.

### Application Areas



### Analysis

Real-time deep packet inspection

### Identification

Automatic identification of OT protocols

### Collection

Collects protocol data in mirroring mode

### Integration

Transmits valuable information to the upper management system

### Conversion

Converts OT protocol data to IT protocol data

### Features & Benefits

- Efficiency**
  - Provides DPI probe function for industrial protocol without changing the network configuration
  - Mirroring mode/unidirectional mode
  - Creates ENTRY for each protocol automatically by mirroring all packets
- Performance**
  - Up to 100,000 PPS processing performance
  - Mirrors and converts OT control data without applying ACL
- Security**
  - Detects and reports forgery and alteration of packets by storing / comparing / analyzing data automatically learned by DPI
  - Alerts security events such as forgeries and abnormal behaviors
  - Unidirectional transmission to the IT system is applicable
- Scalability**
  - Provides automated protocol profiling to facilitate OT protocol extension

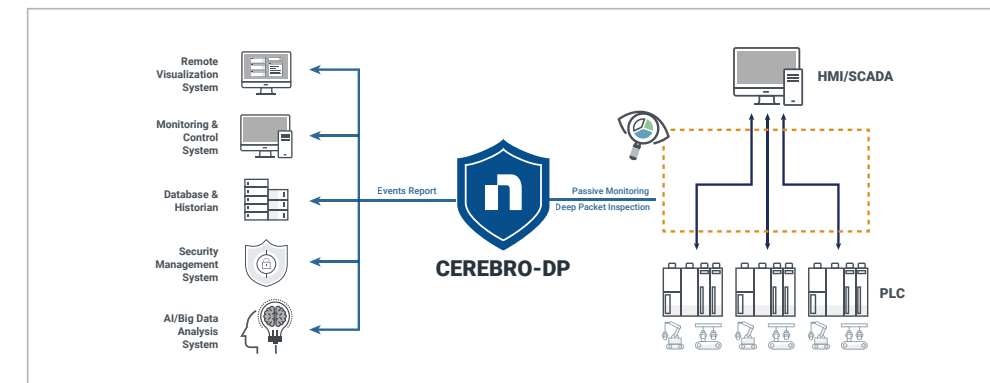
### Supported Protocols

Classification	Protocol	Classification	Protocol
OT Protocols	AutomationDirect	IT Protocols	ODBC
	Cimon		
	EthernetIP		JSON
	Fatek		
	GLOFA-GM, Master-K		SYSLOG
	XGT/XGB/XGI		
	Melsec A Ascii/Binary		XML
	Melsec Q Ascii/Binary		
	ModbusTCP		MQTT
	Omron		
SiemensS7	OPC-UA		
Unitronics			

### Main Functions

Classification	Main Function
Service	Automatically identifies OT protocols based on profiles
	Analyzes and extracts OT protocol data based on profiles
	Converts OT protocols to IT protocols
Security	Detects unauthorized terminals and server access by ACL
	Detects forgery packets based on packet inspection data
	Detects abnormal symptoms based on packet inspection data

### System Structure & Configuration



# ALITA

## Open Architecture Plunger Lift Automation Solution

### OPEN

Open module configuration and standard protocols interworking



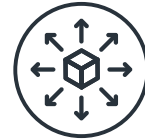
### AUTOMATE

Well automation, remote control and surveillance



### OPTIMIZE

Multi-well control, state synchronization and auto adjustment



**ALITA** is a plunger lift automation solution based on an open architecture that is installed in oil and gas wells using the plunger lift method\*. This solution monitors the condition of the well and automatically controls it 24 hours a day to ensure continuous crude oil/gas production. It monitors the pressure sensors connected to the production pipe and controls the production valve according to the well condition.

To prevent the well from being closed, it is maintained and managed to enable continuous production by continuously removing inhibitory substances such as water and slug. In addition, it enables remote monitoring/control by reporting well status and production history information to the control center in real-time.

\*An artificial lift technology to produce oil and gas

<h4>Automation</h4> <ul style="list-style-type: none"> <li>- Plunger lift control logic and production management</li> <li>- 24/7 control and automatic operation</li> </ul>	<h4>Openness</h4> <ul style="list-style-type: none"> <li>- Decoupling H/W&amp;S/W with open architecture</li> <li>- Interface of standard industrial protocols</li> <li>- Interworking with various sensors &amp; devices</li> </ul>
<h4>Scalability</h4> <ul style="list-style-type: none"> <li>- Docker Container Architecture</li> <li>- Concurrent control and synchronization of Multi-well</li> </ul>	<h4>Convenience</h4> <ul style="list-style-type: none"> <li>- User-defined alarm/control logic</li> <li>- Automatic customization</li> <li>- Remote control and user-oriented dashboard</li> </ul>
<h4>Optimization</h4> <ul style="list-style-type: none"> <li>- Real-time monitoring based on 5G/4G</li> <li>- Optimal control through AI learning</li> <li>- Trend analysis of production and operation</li> </ul>	<h4>Security</h4> <ul style="list-style-type: none"> <li>- Role-based security</li> <li>- Interworking with encrypted data</li> <li>- Access control</li> </ul>

### Supported Protocols

Classification	Protocols
I/O Unit	ModbusTCP
	ModbusRTU
	LSIS XGT Serial
	Mitsubishi Melsec
I/O Sensor	DNP3
	AI/AO ( 4-20mA )
	DI/DO
Flowmeter	ModbusTCP
	ModbusRTU
SCADA	ModbusTCP
	OPC-UA
Others	MQTT

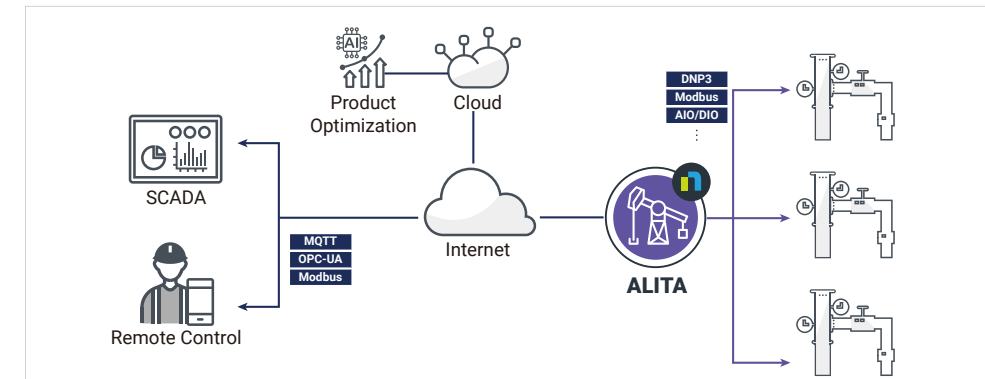
### Features & Benefits

<b>Open Platform</b>	<ul style="list-style-type: none"> <li>• Improves compatibility through modularization of RTU units</li> <li>• Reduces replacement/substitution costs by configuring a universal/open platform</li> <li>• Provides interworking between various heterogeneous systems through standard protocol interfaces</li> </ul>
<b>Operational Efficiency</b>	<ul style="list-style-type: none"> <li>• Improves independence of control by separating control logic and user interface</li> <li>• Provides various information for system surveillance, analysis, and optimization</li> <li>• Enhances security with the function of setting permissions by user roles</li> <li>• Includes remote control/surveillance through 5G/4G modem</li> </ul>
<b>Automatic Control</b>	<ul style="list-style-type: none"> <li>• Monitors wells for 24/7 and control production automatically</li> <li>• Adjust of automatic production according to well environment</li> <li>• Concurrent Multi-well control and synchronize state of wells</li> <li>• Monitors the environment of wellhead and operate well optimally</li> </ul>

### Main Functions

Classification	Main Functions	Contents
Plunger	Multi-well Control	Control and surveillance of Multi-well in a single RTU
	Well Synchronization	Efficient Wellpad operation through state synchronization among plunger lifts
	User Defined Logic	Optimized operation for various well environments by controlling plunger lift logic according to user definition
	PID Control	Supports analog valve through PID control
Security	Secured Communication	Improved security through encrypted data communication
	Role-based Security	Management of level and restrict system operation by user role
GUI	Dashboard	Monitoring on production and state information in real-time
	I/O Unit	Interworks with Modbus protocol to recognize and drive heterogeneous I/O modules(analog/digital)
Device	SCADA	Supports standard industrial control protocol(Modbus, OPC-UA, MQTT etc.) for industrial IoT
	Flow Computer	Modbus protocol Interworking and time synchronization
	Auto Adjustment	Production optimization and auto tuning according to field conditions
Optimization	PID Learning & Tuning	Optimal PID based on AI

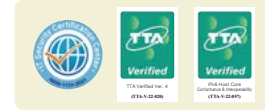
### System Structure & Configuration



# VIPER-N

## VoIP Security Gateway Solution

\*VoIP (Voice over Internet Protocol)



### Korea No.1 VoIP Security Solution

Since

**2008**

Korea Army Market Share

**96%**

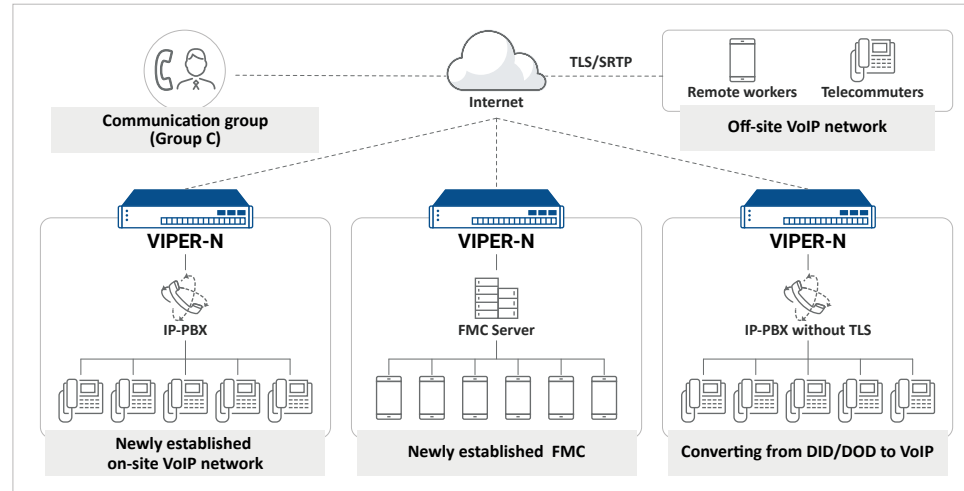
Public Institutions References

**200+**



VIPER-N is a security gateway exclusively for VoIP, which detects and blocks security attacks on VoIP in advance by monitoring the traffic flowing into the company.

It is an **ALL-IN-ONE appliance device** that provides the NAT traversal processing for FMC/UC, topology hiding to protect address information in the company, and the encryption of RFC3261 SIP traffic altogether.



### Features

<b>VoIP Security</b>	<ul style="list-style-type: none"> <li>· Detects and blocks VoIP security threats                     <ul style="list-style-type: none"> <li>✓ Abnormal messages (more than 40,000 messages)</li> <li>✓ SIP/RTP/TCP/ICMP Flooding</li> <li>✓ Dos/DDos, Abnormal sessions</li> </ul> </li> <li>· Controls access of unauthorized terminals (Static/Dynamic ACL)</li> <li>· Protects address information in the company (Topology Hiding)</li> </ul>
<b>User Convenience</b>	<ul style="list-style-type: none"> <li>· Possible to operate by changing between SBC type and IPS type</li> <li>· Guarantees seamless service with a redundant configuration                     <ul style="list-style-type: none"> <li>✓ Active-Standby redundant configuration</li> </ul> </li> <li>· Possible to extend software license                     <ul style="list-style-type: none"> <li>✓ Based on subscriber/simultaneous call capacity</li> </ul> </li> <li>· Provides a web-based (HTTPS) management page</li> </ul>
<b>Encryption</b>	<ul style="list-style-type: none"> <li>· TLS V1.2/1.0 applied</li> <li>· Encryption standard protocol AES/ARIA</li> <li>· Conversion between protocols ( UDP ↔ TCP / UDP ↔ TLS / TCP ↔ TLS )</li> </ul>
<b>NAT Traversal</b>	<ul style="list-style-type: none"> <li>· VoIP ALG for NAT/firewall traversal</li> <li>· Accepts IP-PBX and VoIP terminals using private IP</li> <li>· Supports SIP connect/trunking</li> </ul>
<b>Compliance</b>	<ul style="list-style-type: none"> <li>· Korea Common Criteria EAL 3</li> <li>· TTA Verified Ver.4 certified</li> <li>· TTA IPv6 Host Core Conformance &amp; Interoperability certified</li> </ul>

### Product Specifications

Details	VIPER-N		
Type	SOHO	Enterprise	Exclusive for FMC
<b>Appliance</b>			
<b>Simultaneous calls</b>	30 ~ 60 calls	100 ~ 8,000 calls	100 ~ 8,000 calls
<b>Registered subscribers</b>	300 ~ 600	1,000 ~ 80,000	1,000 ~ 80,000
<b>Processor</b>	Intel Quad-Core 2.2GHz	Intel Quad-Core 3.1GHz	Intel Quad-Core 3.1GHz
<b>Memory</b>	4G	8G	8G
<b>HDD</b>	500G	1TB	1TB
<b>Network Interface</b>	4* 10/100/1000	4* 10/100/1000	4* 10/100/1000
<b>Support IPv6</b>	✓	✓	✓
<b>Encryption</b>	Signaling : TLS V1.2/1.0 Media : SRTP	Signaling : TLS V1.2/1.0 Media : SRTP	Signaling : TLS V1.2/1.0 Media : SRTP
<b>Encryption Algorithm</b>	AES, ARIA	AES, ARIA	AES, ARIA
<b>Key Exchange</b>	RSA, ECC	RSA, ECC	RSA, ECC
<b>Power</b>	Single AC	Single or Redundant AC or DC	Single or Redundant AC or DC

\* The server may change due to the manufacturer's circumstances



## References

### Smart Monitoring System (Eco Delta City)

- CEREBRO-C in Water Facilities Monitoring System
- collecting water facilities data in real-time
  - linking the monitoring system (SAMSUNG SDS Brightics IoT) and the water facilities

### Hydrogen Refueling Stations Control System

- CEREBRO-C in Remote Control System for Hydrogen Stations
- collecting operation data of hydrogen refueling stations
  - linking the remote control system (OPC-UA) and the hydrogen refueling station SCADA (ModbusTCP)

### Automobil Manufacturing

- CEREBRO-DP in Smart Factory
- providing OT networks and assets visibility
  - detecting continuously OT networks security threats, such as control data code forgeries
  - offering the basement for vulnerability and risk management

## References

### Building Management System (IDC)

- CEREBRO-DD in IDC Management System
- unidirectionally transmitting building data (SNMP) to the management system (Modbus)
  - protecting the database system from the external security threats including unauthorized access


### CCTV Monitoring System (Power Plant)


- CEREBRO-DD in Video Surveillance System
- unidirectionally transmitting CCTV data (RTSP/RTP) to SCADA for video surveillance (ModbusTCP)
  - protecting OT networks in the power plant from the external security attacks

### Public Institution VoIP Network

- VIPER-N in City Hall VoIP Network
- blocking DoS/DDoS attacks on VoIP gateway
  - changing the public IP of the gateway to a private IP
  - preventing abnormal behaviors from the gateway

## NAONWORKS Co., LTD.

 : Rm711, 271, Digital-ro, Guro-gu, Seoul, Korea (H.Q)  
: A-301, 240, Pangyoyeok-ro, Bundang-gu,  
Seongnam-si, Gyeonggi-do, Korea (2nd R&D Center)

 : +82 2-2025-1630

 : sales@naonworks.com

 : www.naonworks.com

