Monitoring Production (OT) Environments Using Zabbix Technology

Who am I

Ari Rajamäki, Product Manager, Cybersecurity

Ari is Product Manager for Cybersecurity in Valmet - a leading global developer and supplier of process technologies, automation and services for the pulp, paper and energy industries.

- ✓ Zabbix Summit 2022 table hockey Champion

- ✓ Cyber security Engineer, Master of Engineer at JAMK University of Applied Sciences 2021
- ✓ GICSP (Global Industrial Cyber Security Professional), GIAC Certification 2019 Cyber Security Certifications | GIAC Certifications
- ✓ Certification 2023 ISA/IEC 62443 Cybersecurity Fundamentals Specialist (CFS) Certification 2022 ISA/IEC 62443 CSF Certificate 1
- ✓ ISA/IEC 62443 Cybersecurity Risk Assessment Specialist ISA/IEC 62443 CRAS - Certificate 2

Industrial Automation and Control System monitoring in different industries and environments

Pulp and paper

Risk of losing money, risks against personnel safety and environment hazards

Threats from cybercriminal adversary groups from stealing (industry espionage) the business-critical or GDPR protected data.

Threats from cybercriminal to crypt your data and lock systems via ransomware campaigns

Energy

Risks against money, personnel and environment safety

Similar and new threats form government funded groups.

More complex threats from cybercriminals government funded adversary to crypt/wipe your data, lock system to create society hazards and weakening the critical infrastructure

Marine

Risks against money, personnel and environment safety

Similar threats lands scape with industry unique risks and consequences

Challenging environment to protect, response and recover. Connectivity, resources and skills onboard are limited

Process industries

Risks against money, personnel and environment safety

Similar threats lands scape with high consequences

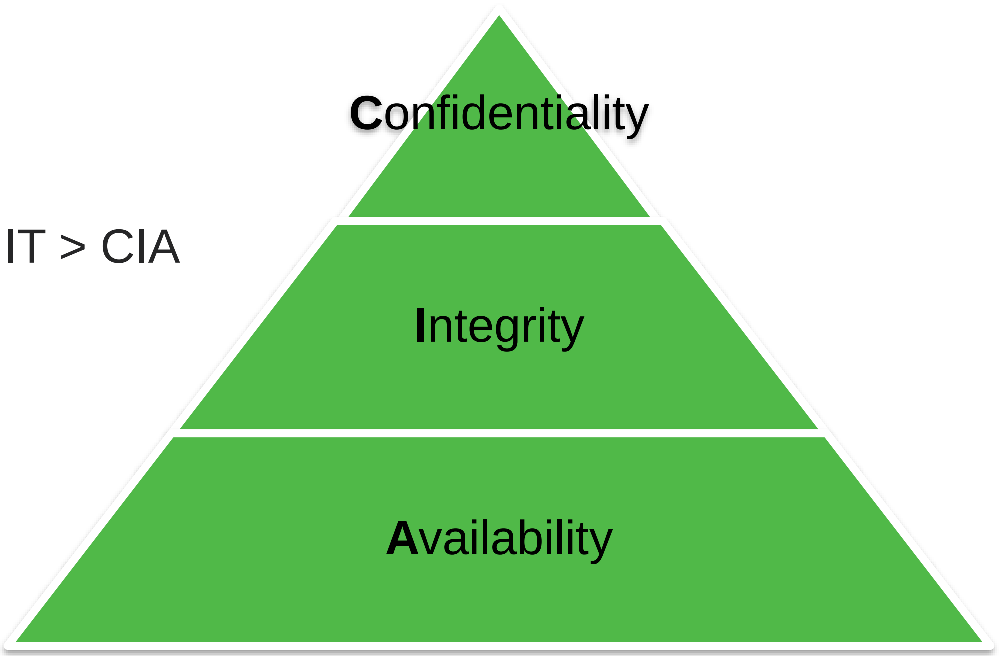
Same cybersecurity risk mitigation strategies applies. All steps taken improves resilience's of loosing control of production process during cyber attack

Industrial Control System meets IT information security

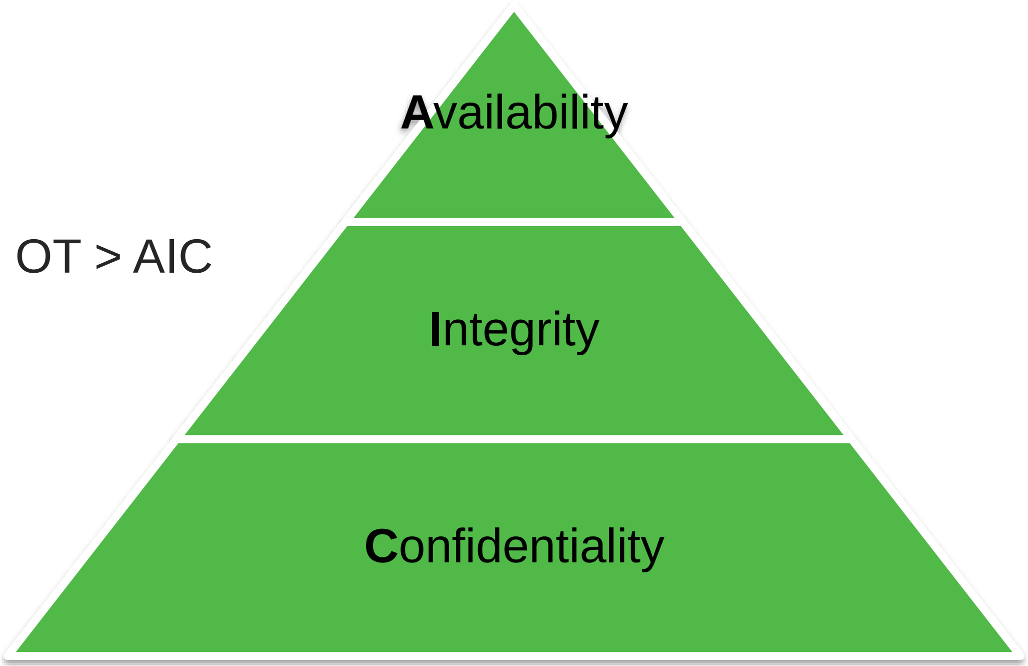
IT Information Technology vs. OT Operational Technology

CIA Triad model for information security priority is reversed in OT and availability of control system is critical to stable and working process

IT > CIA



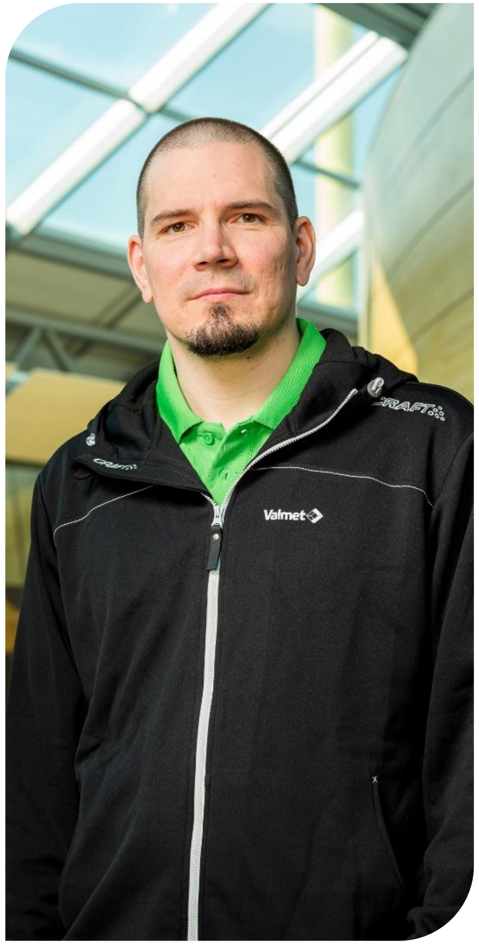
OT > AIC



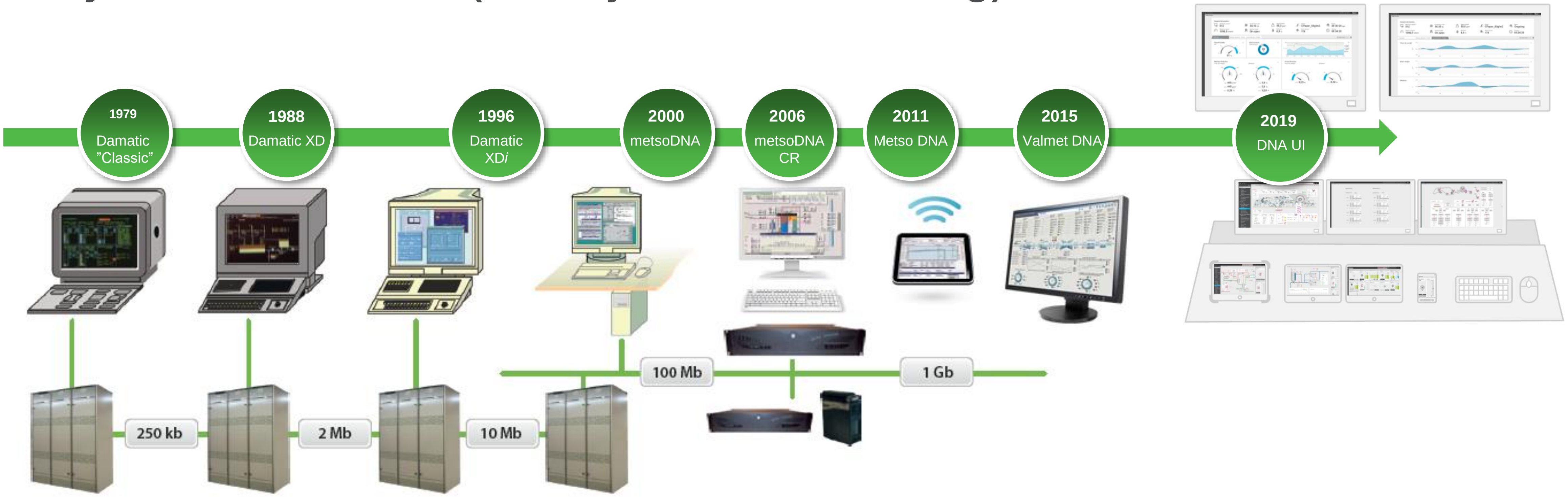
In OT Availability is still the king and this is why we are monitoring ICS assets using Zabbix...

Who am I

- Mikko Tikkala, Senior Specialist, Cyber Security Services at Valmet
- Zabbix Summit 2022 table hockey silver medalist 🥈
- MEng (Automation technology), GICSP, Zabbix 6.0 Certified Expert
- Zabbix hobbyist



History of Valmet DNA (and system monitoring)



Internal system diagnostics

Internal system diagnostics + Nagios Core

Internal system diagnostics + Zabbix

Finding successor for Nagios

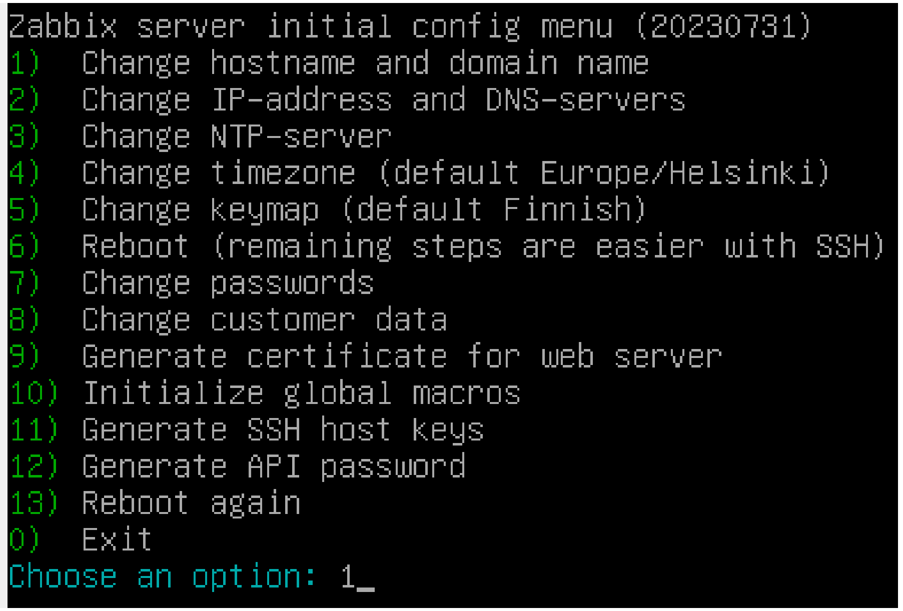
- Masters' thesis was started at 2017 to find successor for Nagios
- Things to consider
  - ✓ Security
  - ✓ Regular updates
  - ✓ Scalability
  - ✓ Flexibility
  - ✓ Licensing costs
- Of course, the answer for these requirements is Zabbix!
- 1st customer pilots were made in 2018
- Nowadays there are a few dozen of Zabbix instances all over the world
- There is huge grow potential, because Valmet has delivered 1500+ systems

Valmet way to use Zabbix

- Smaller customer sites can use Zabbix server located at public cloud
- Bigger sites has on-prem Zabbix server
- One virtual machine template which includes all needed
  - Applications
  - Configuration scripts
  - Valmet templates
  - Sample configurations
- Offline upgrade kits are made with apt-offline. So, every Zabbix instance can be patched even they are in dark sites.
- Problem indications over SMTP

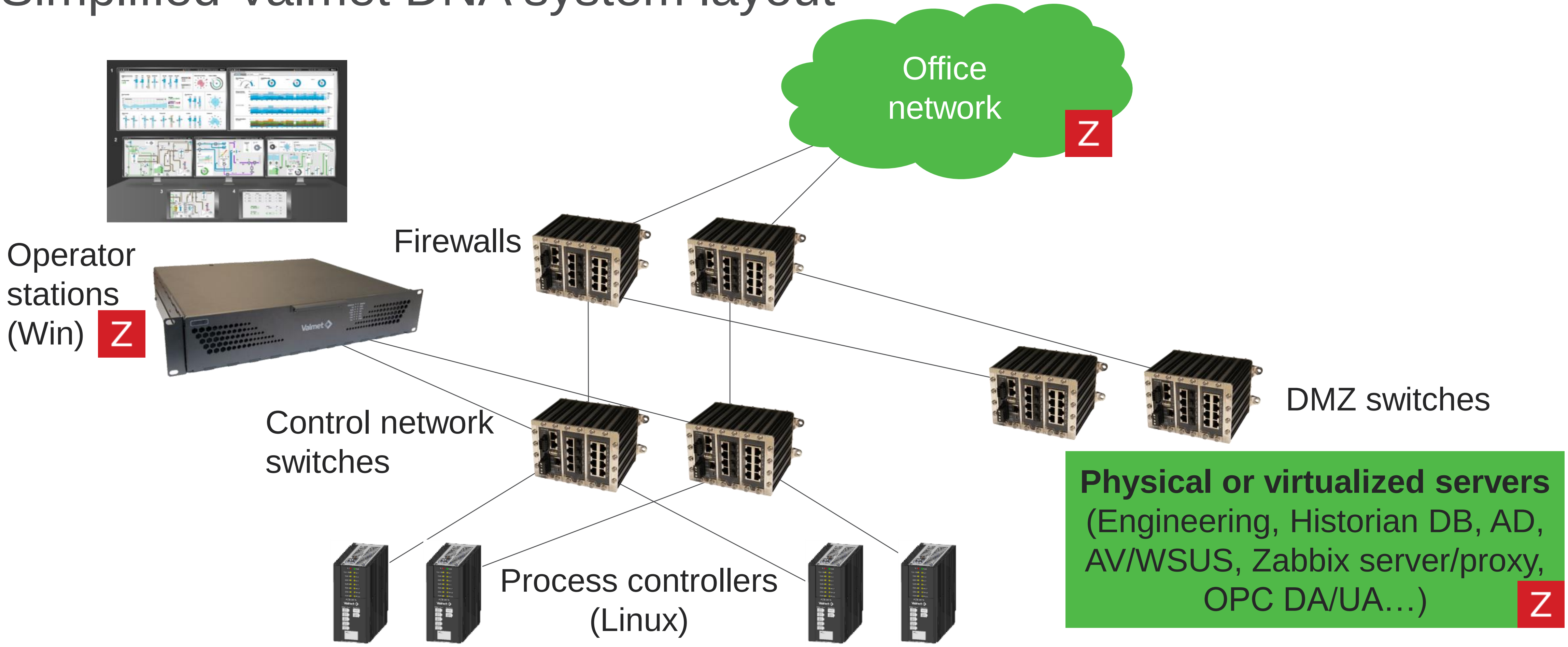
Zabbix deployment

- Initial config script is all what needs to be done from Linux command line
- Script configures hostname, IP-address, etc.
- Script generates agent configuration files with encryption settings to Zabbix server
- Agents can be deployed to target machines by script
- Agents are using auto registration
- API script can be used for mass operations, if user does not want to add SNMP devices manually from Zabbix UI



```
Zabbix server initial config menu (20230731)
1)  Change hostname and domain name
2)  Change IP-address and DNS-servers
3)  Change NTP-server
4)  Change timezone (default Europe/Helsinki)
5)  Change keymap (default Finnish)
6)  Reboot (remaining steps are easier with SSH)
7)  Change passwords
8)  Change customer data
9)  Generate certificate for web server
10) Initialize global macros
11) Generate SSH host keys
12) Generate API password
13) Reboot again
0)  Exit
Choose an option: 1_
```

Simplified Valmet DNA system layout



Office network Z

Operator stations (Win) Z

Firewalls

DMZ switches

Control network switches

Process controllers (Linux)

Physical or virtualized servers (Engineering, Historian DB, AD, AV/WSUS, Zabbix server/proxy, OPC DA/UA…) Z

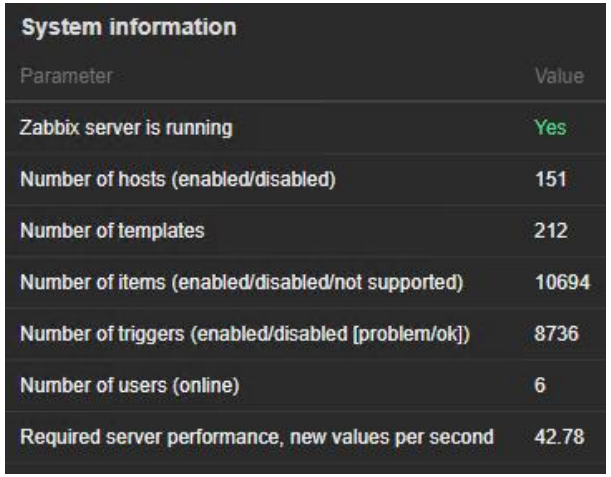
Valmet DNA I/O, Fieldbuses (Profinet, Profibus…), **Interfaces** (IEC, Modbus…)

Field devices (motors, pumps, valves, sensors, analyzers…)

Some customer cases

Process industry customer

- Network monitoring

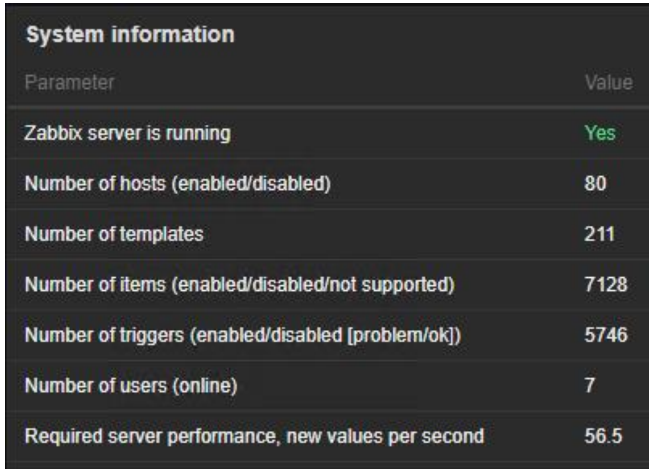


System information

Parameter	Value
Zabbix server is running	Yes
Number of hosts (enabled/disabled)	151
Number of templates	212
Number of items (enabled/disabled/not supported)	10694
Number of triggers (enabled/disabled [problem/ok])	8736
Number of users (online)	6
Required server performance, new values per second	42.78

Power industry customer

- Full system monitoring

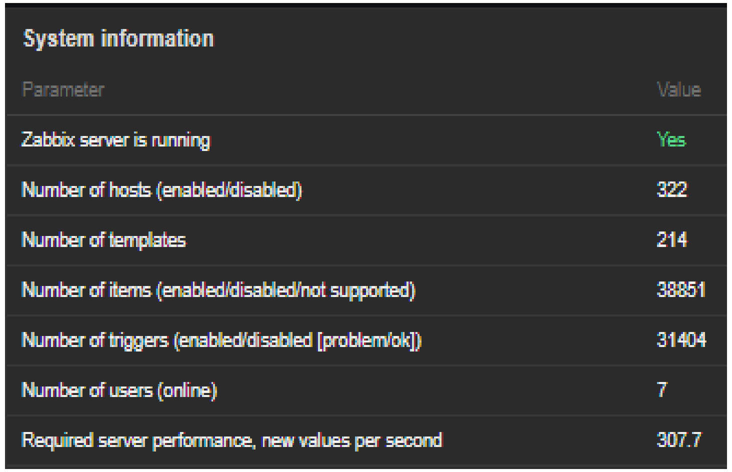


System information

Parameter	Value
Zabbix server is running	Yes
Number of hosts (enabled/disabled)	80
Number of templates	211
Number of items (enabled/disabled/not supported)	7128
Number of triggers (enabled/disabled [problem/ok])	5746
Number of users (online)	7
Required server performance, new values per second	56.5

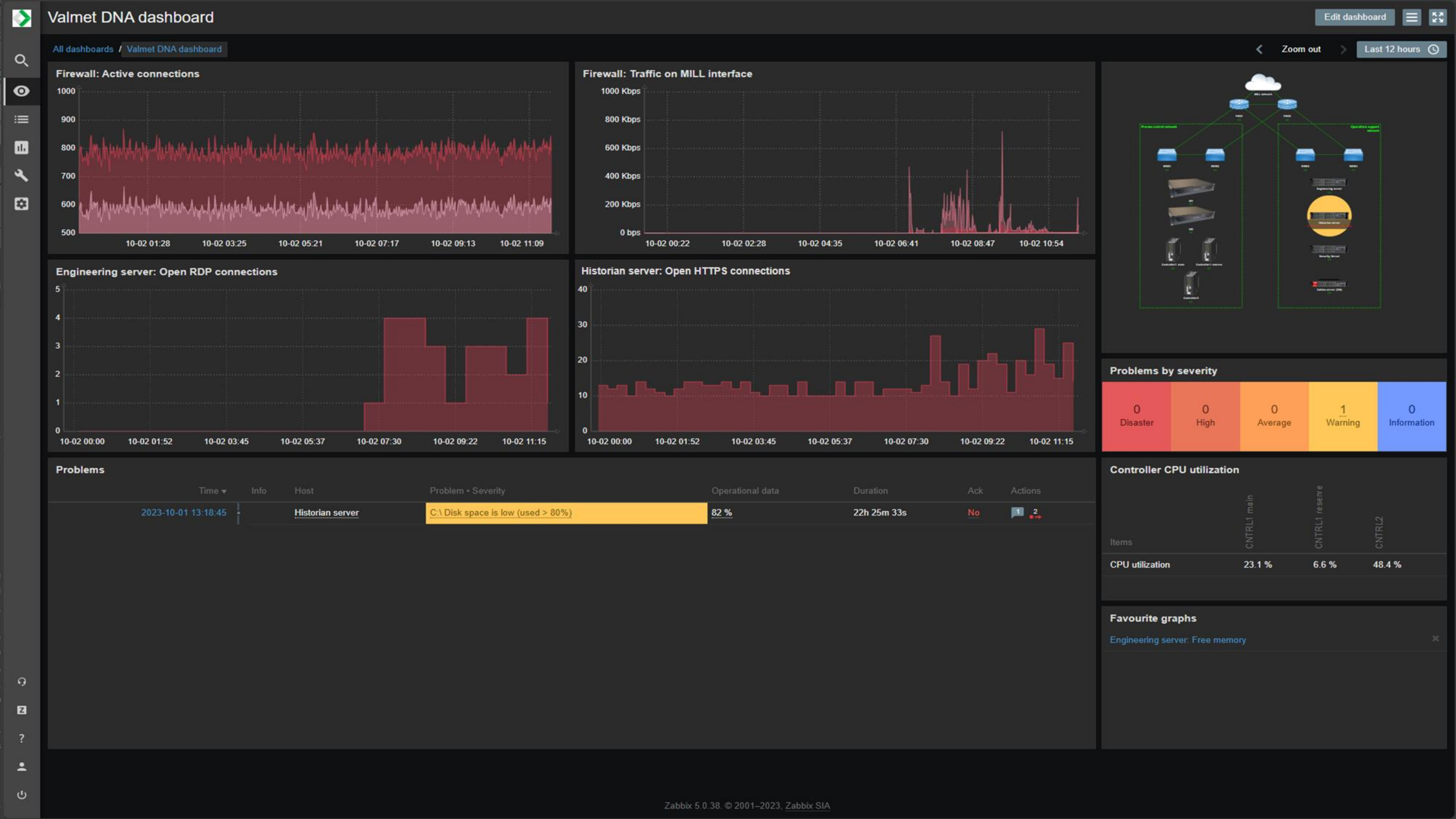
Pulp/paper industry customer

- Full system monitoring



System information

Parameter	Value
Zabbix server is running	Yes
Number of hosts (enabled/disabled)	322
Number of templates	214
Number of items (enabled/disabled/not supported)	38851
Number of triggers (enabled/disabled [problem/ok])	31404
Number of users (online)	7
Required server performance, new values per second	307.7



Problems by severity

0 Disaster	0 High	0 Average	1 Warning	0 Information

Problems

Time ▾	Info	Host	Problem • Severity	Operational data	Duration	Ack	Actions
2023-10-01 13:18:45		Historian server	C:\ Disk space is low (used > 80%)	82 %	22h 25m 33s	No	2

Controller CPU utilization

Items	CNTRL1 main	CNTRL1 reserve	CNTRL2
CPU utilization	23.1 %	6.6 %	48.4 %

Favourite graphs

Engineering server: Free memory

Zabbix 5.0.38. © 2001–2023, Zabbix SIA

Global presence - close to customers

EMEA

20 R&D centers
86 service centers
24 production units
76 sales offices
Head office

👤 10,787

NET SALES EUR MILLION 1,876

NORTH AMERICA

3 R&D Centers
29 service centers
17 production units
11 sales offices

👤 2,040

NET SALES EUR MILLION 1,058

SOUTH AMERICA

5 service centers
1 production units
8 sales offices

👤 833

NET SALES EUR MILLION 718

CHINA

3 R&D Centers
5 service centers
6 production units
6 sales offices

👤 2,323

NET SALES EUR MILLION 829

ASIA-PACIFIC

2 R&D Centers
11 service centers
6 production units
29 sales offices

👤 1,565

NET SALES EUR MILLION 593

Valmet in total:

- >130 service centers
- >50 production units
- 28 R&D centers

Automation Systems:

- 2,050 automation professionals
- 590 service engineers
- 630 own operations professionals

Valmet

FORWARD