IT Infrastructure tips & tricks for Control System and PLC

SOLARIS
Michał Ostoja-Gajewski

Introduction

- ✓ Kraków, Poland
- ✓ SOLARIS is a part of CERIC-ERIC
- ✓ Active network ports > 1000
- ✓ Virtual Machines > 150
- ✓ Tech:
  - ✓ Extreme Networks
  - ✓ Juniper
  - ✓ Fortinet
  - ✓ Dell
  - ✓ VmWare 6.5
  - ✓ Solarwinds
  - ✓ Flowmon
- ✓ Solaris total staff : ~ 50

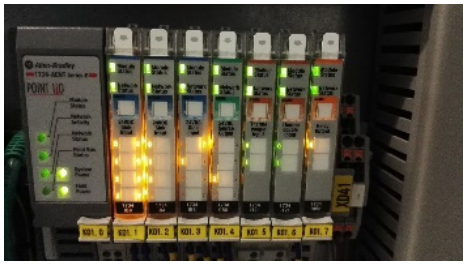
- ✓ SOLARIS is a little brother of MAX IV
- ✓ Linac, 1.5 GeV Ring ready
- ✓ Beamlines:
- PEEM/XAS commissioning
- UARPES commissioning
- PHELIX construction started
- XMCD construction started
- 4 beamlines in pipeline

Real life scenarios

1. Machine Protection System - PLC network
2. Traffic separation based on device type
3. Device – Device Server – Control Room
4. Diagnostics devices - traffic producers
5. Traffic flow based monitoring
6. Local network issues diagnostics with TAP

Machine Protection System – PLC network

- MPS based on Rockwell Automation PLC



- RA CPUs communicating with IOs using dedicated vlans (e.g. plc-linac) in common network

- CPU <--> IO communication in 20ms cycle (CPU sends request, IO processes data, IO sends response)

- In case of lost communication between CPU and IO, interlock stops entire machine

Machine Protection System – PLC network

- Bad approach : PLC traffic aggregated with other traffic in shared FO 1GBit/s links

- Random „lost communication” interlocks on PLC IO modules due to bursty traffic from other sources and possible congestion. No help from prioritizing traffic.

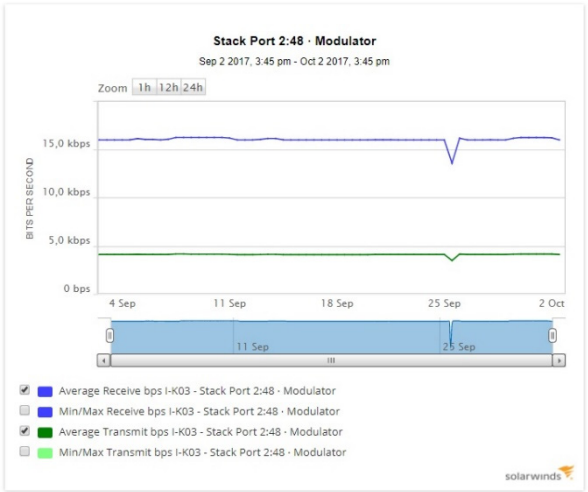
✓ **TIP:** make separate FO connections and dedicated network switches for interconnecting PLC CPUs and IOs
✓ Result: No further interlocks observed

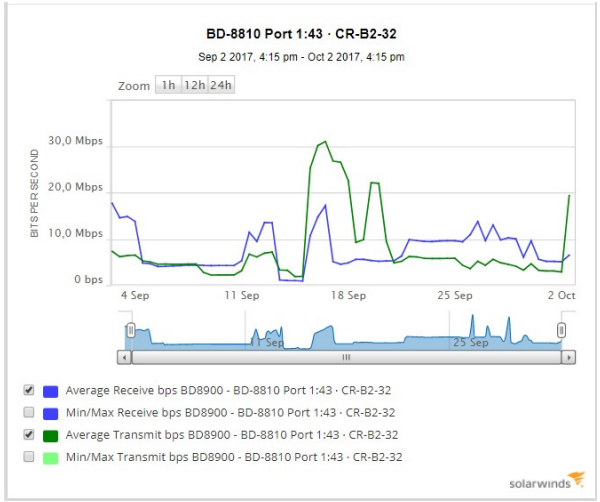
Traffic separation based on device type

- Multiple types of devices attached to network
    - Power supplies for magnets
    - Ion pumps controllers
    - Scopes, diagnostics systems
    - RF systems
    - Timing system
    - PLC
- Multiple Tango9 device servers running on virtual machines

Traffic separation based on device type

- Ion Pump Controller and Modulator in I-K03 section
- Control Room workstation





Traffic separation based on device type

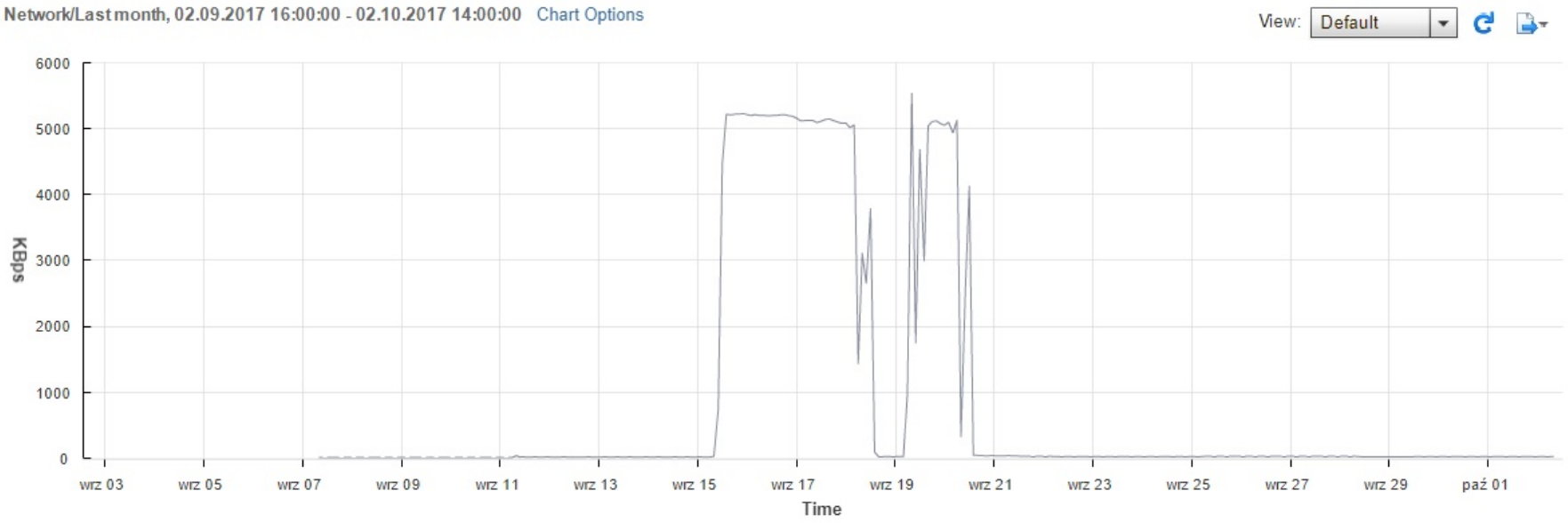
- T9-RF-RING virtual machine traffic

Performance Chart Legend

Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
■	T9-RF-RING	Usage	Average	KBps	154	3135	18	363.98

Traffic separation based on device type

- T9-DIA-CAM virtual machine traffic



Performance Chart Legend

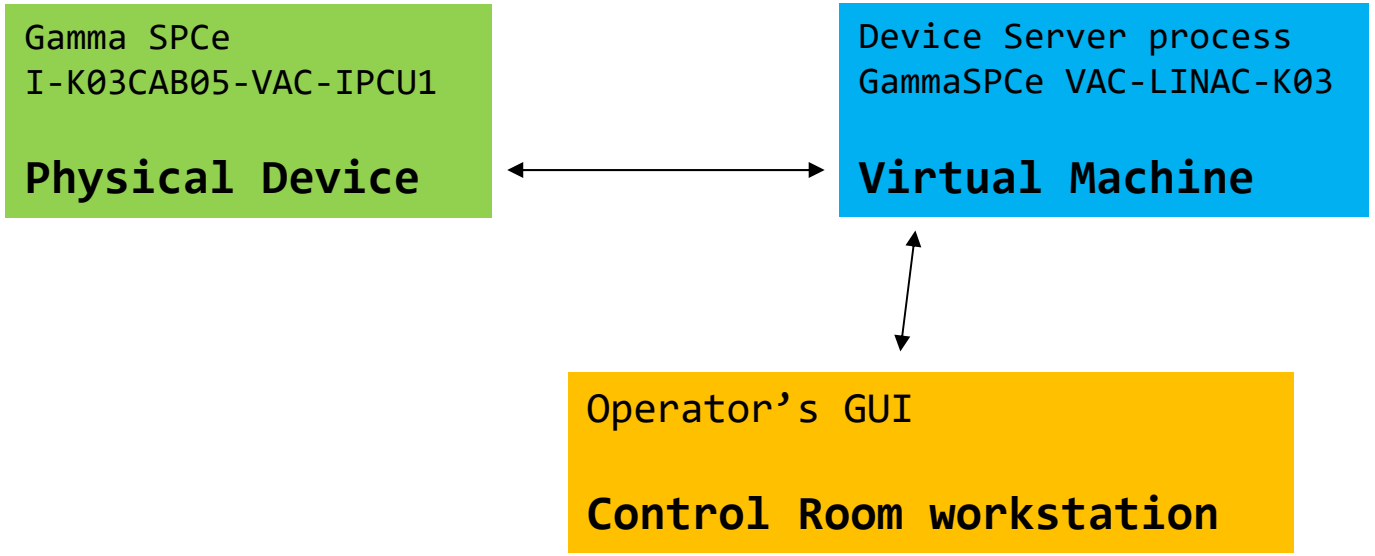
Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
■	T9-DIA-CAM	Usage	Average	KBps	24	5537	13	831.807

Traffic separation based on device type

- ✓ **TIP:** make the logical separation using 802.1q vlans for each subsystems. Example: vac-linac, mag-linac, rf-linac, dia-linac, vac-ring etc.
- ✓ **TIP:** Attach virtual machines with Tango9 devices servers to the same vlan as controlled subsystem
- ✓ Result: Better control of traffic patterns and isolation of possible issues

Device <-> Device Server <-> Control Room

- Devices (e.g. power supplies) exchange traffic with Tango9 device servers running on virtual machines
- Operator's Tango9 apps run on control room workstations communicating with device servers



- Tango9 apps use polling or event based communication implementing publish/subscribe pattern

Device <-> Device Server <-> Control Room

✓ **TIP:** make the shortest logical and physical network path between device servers and GUI apps

Operator@CR2:~

```
[Operator@CR2 ~]$ ping vac-linac.m.cps.uj.edu.pl
PING vac-linac.m.cps.uj.edu.pl (192.168.133.20) 56(84) bytes of data.
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=1 ttl=63 time=0.228 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=2 ttl=63 time=0.199 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=3 ttl=63 time=0.292 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=4 ttl=63 time=0.205 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=5 ttl=63 time=0.159 ms
^C
--- vac-linac.m.cps.uj.edu.pl ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.159/0.216/0.292/0.046 ms
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$ traceroute vac-linac.m.cps.uj.edu.pl
traceroute to vac-linac.m.cps.uj.edu.pl (192.168.133.20), 30 hops max, 60 byte packets
 1  192.168.130.4 (192.168.130.4)  0.839 ms  0.892 ms  0.978 ms
 2  vac-linac.m.cps.uj.edu.pl (192.168.133.20)  0.196 ms  0.184 ms  0.170 ms
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
```

Device <-> Device Server <-> Control Room

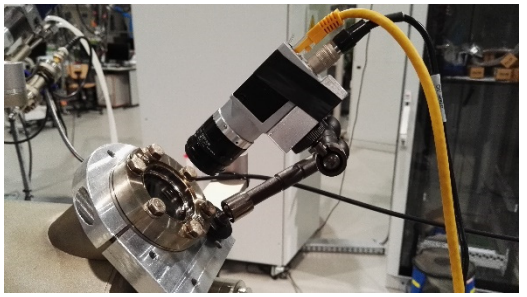
- ✓ **TIP:** make the shortest network path between VM with device servers and physical devices

admin@vac-linac:~

```
[admin@vac-linac ~]$ hostname
vac-linac.m.cps.uj.edu.pl
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$ ping 192.168.133.110
PING 192.168.133.110 (192.168.133.110) 56(84) bytes of data.
64 bytes from 192.168.133.110: icmp_seq=1 ttl=64 time=0.256 ms
64 bytes from 192.168.133.110: icmp_seq=2 ttl=64 time=0.200 ms
64 bytes from 192.168.133.110: icmp_seq=3 ttl=64 time=0.248 ms
64 bytes from 192.168.133.110: icmp_seq=4 ttl=64 time=0.222 ms
^C
--- 192.168.133.110 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.200/0.231/0.256/0.026 ms
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$ traceroute 192.168.133.110
traceroute to 192.168.133.110 (192.168.133.110), 30 hops max, 60 byte packets
 1  I-K03CAB05-VAC-IPCU1.vaclin.m.cps.uj.edu.pl (192.168.133.110)  0.214 ms  0.249 ms  0.204 ms
[admin@vac-linac ~]$
[admin@vac-linac ~]$
```

Diagnostics devices – huge traffic producers

- Example: Bassler cameras producing huge traffic during beamline conditioning



- Default settings:
  - Resolution: 1280x1024
  - Bits per pixel: 12 (in real: 16bits)
  - FPS: no limit (in real: 40)
  - Traffic: ~ 900 MBit/s

- Pylon or LimaCCDs Tango9 device server are used to manage 5 cameras during conditioning

Diagnostics devices – huge traffic producers

- Problem: huge traffic volume can not be handled correctly by 1Gbit interface and apps on beamline workstation

✓ **TIP:** Reduce traffic by setting acceptable quality parameters:

- ✓ Resolution: 640x512
- ✓ Bits per pixel: 8
- ✓ FPS: limit : 25
- ✓ Traffic: ~65 MBit/s

✓ **TIP:** Enable Jumbo frames (mtu:9000) for bigger resolutions to get smooth camera view

Flow based monitoring

- Each communication between two network attached devices can be regarded as flow

Start Time - first seen	Duration	Protocol	Source IP address	Source port	Destination IP address	Destination port	TCP Flags	TOS	Packets	Bytes	Packets per second	Bits per second	Bytes per packet	Flows
2017-09-28 13:47:32.877	0.002 s	TCP	c2.bl04.cps.uj.edu.pl	46966	hdbplus-cass.bl04.cps.uj.edu.pl	45266	...AP.S.	Best Effort & Default	36	37460	18000	149.8 M	1040	1
2017-09-28 13:48:44.642	0.015 s	TCP	plc.bl04.cps.uj.edu.pl	53805	vac.bl04.cps.uj.edu.pl	35440	...AP.S.	Best Effort & Default	168	235692	11200	125.7 M	1402	1

- Flows can vary in duration, traffic volume, usage of multiple ports

- Networking devices can produce information on flows and send it to flow collector via NetFlow, IPFIX, sFlow or jFlow protocols

Flow based monitoring

- NetFlow v9 and IPFIX are most popular protocols for traffic flow base monitoring

- Tango9 based control system generates multiple flows : device servers talkig to devices, gui apps talking to device servers, archiving systems polling for data etc.

✓ **TIP:** use flow monitoring software to analyze Tango9 flows and identify error-prone parts of system

✓ **TIP:** use Anomaly Detection Systems to identify deviations from „normal” traffic

Flow based monitoring – Anomally Detection

- Example of unsucessfull connections between control room workstations and timing system event receiver – topic for further investigation

192.168.143.121 (unknown) 1 threats

192.168.143.113 (unknown) 2 threats

Unavailable services: TCP/58767 (not specified). Time: 2017-09-27 18:35:00 - 2017-09-28 00:35:00, Closed

#	Source	Event type	Detail	Timestamp	Flow source	Targets
1	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 4, rejected connections: 104. Successful traffic - clients: 0, connections: 0.	2017-09-28 00:35:00	Default	192.168.130.13 (unknown), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl)
2	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 169. Successful traffic - clients: 0, connections: 0.	2017-09-27 22:30:00	Default	192.168.105.111 (unknown), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl), 192.168.130.13 (unknown), 192.168.130.11 (cr2.m.cps.uj.edu.pl)
3	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 129. Successful traffic - clients: 0, connections: 0.	2017-09-27 22:25:00	Default	192.168.105.111 (unknown), 192.168.130.13 (unknown), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl)
4	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 114. Successful traffic - clients: 0, connections: 0.	2017-09-27 19:30:00	Default	192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.105.118 (unknown), 192.168.130.13 (unknown), 192.168.130.18 (cr8.m.cps.uj.edu.pl)
5	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 109. Successful traffic - clients: 0, connections: 0.	2017-09-27 19:20:00	Default	192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.105.118 (unknown), 192.168.130.18 (cr8.m.cps.uj.edu.pl), 192.168.130.13 (unknown)
6	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 6, rejected connections: 110. Successful traffic - clients: 0, connections: 0.	2017-09-27 18:35:00	Default	192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl), 192.168.130.13 (unknown), 192.168.105.120 (unknown), 192.168.105.118 (unknown)

Unavailable services: TCP/58767 (not specified). Time: 2017-09-27 13:50:00 - 13:50:00, Closed

Local network diagnostics with TAP

- Network issues can be tracked in place where device is attached by using port mirroring / SPAN to monitor traffic with e.g. Wireshark

- Port mirror/SPAN do not replicate corrupted frames, so not all traffic can be seen

✓ **TIP:** use network TAP between device and switch and monitor entire traffic including malformed frames

Quick Summary

- **TIP:** Monitor, analyze and understand your traffic
- **TIP:** Redesign your network infrastructure to comply with your traffic patterns

SOLARIS NATIONAL SYNCHROTRON RADIATION CENTRE
michal.ostoja-gajewski@uj.edu.pl
https://linkedin.com/in/michal-ostoja-gajewski