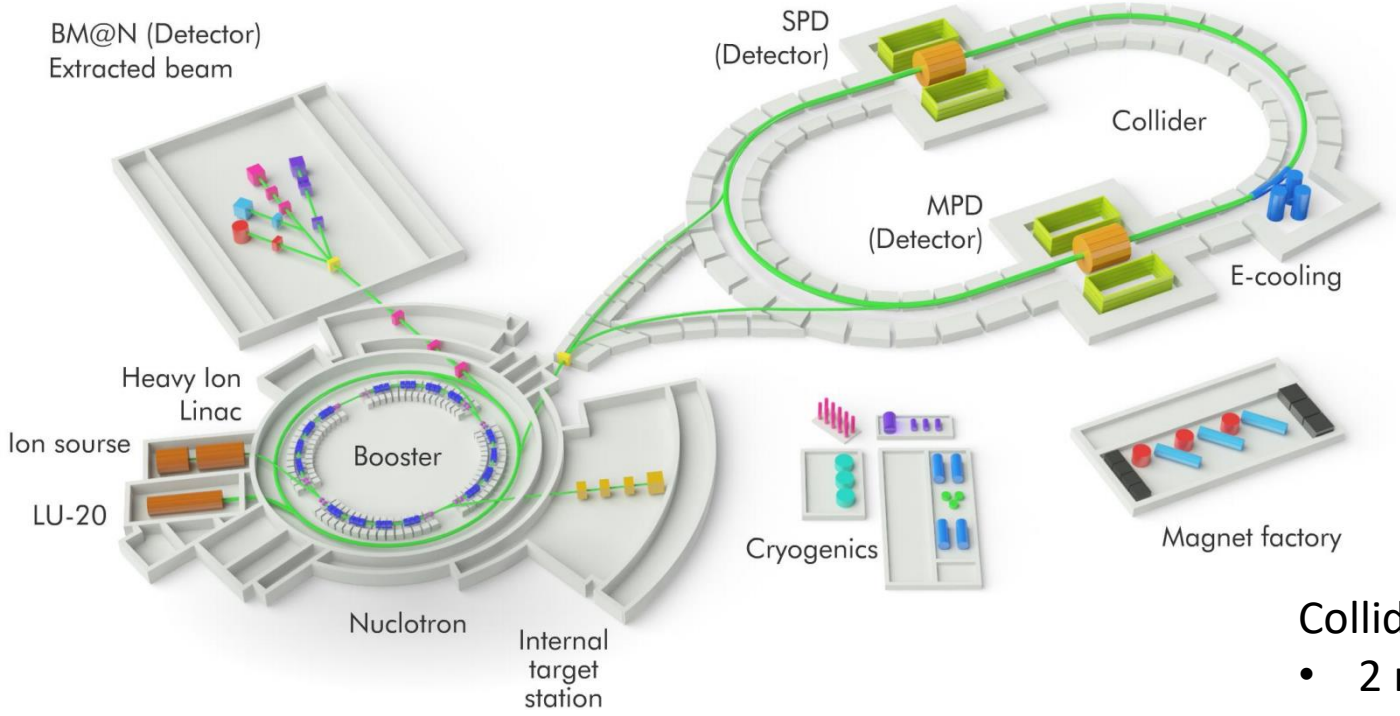
The Nuclotron and NICA Control System

Evgeny Gorbachev on behalf of team LHEP, JINR

Content

- NICA complex
- Main principles and layout.
- Control System infrastructure and services:
  - High availability and scalability.
  - Monitoring
  - Access control and logging.

NICA accelerating complex



- Injection complex
- new superconducting Booster synchrotron
- existing superconducting heavy ion synchrotron Nuclotron
- collider having two new superconducting storage rings
- new beam transfer channels

Collider parameters:

- 2 rings
- 22 bunches Au^{79+}
- $2 \cdot 10^9$ ions in a bunch
- 4.5 GeV/n Au^{79+}
- $L=10^{27}$ $cm^{-2} \cdot c^{-1}$

NICA accelerating complex

2019:

Stage I: Experiment “The Baryonic Matter at Nuclotron”

- Injection complex: KRION, HILAc, LU20
- Booster
- BT Line Booster – Nuclotron
- Nuclotron upgraded
- BM@N Detector setup

2020:

Stage II-a: The basic configuration of the NICA complex

- BT Line Nuclotron => Collider
- Collider:
- Collider RF systems in a reduced version
- Stochastic cooling system – 1 channel per ring
- Multi-Purpose Detector (MPD) in a reduced version: no Inner Tracker System (ITS)

2023:

Stage II-b: The full (project) configuration of the NICA complex

- Collider and MPD in full version

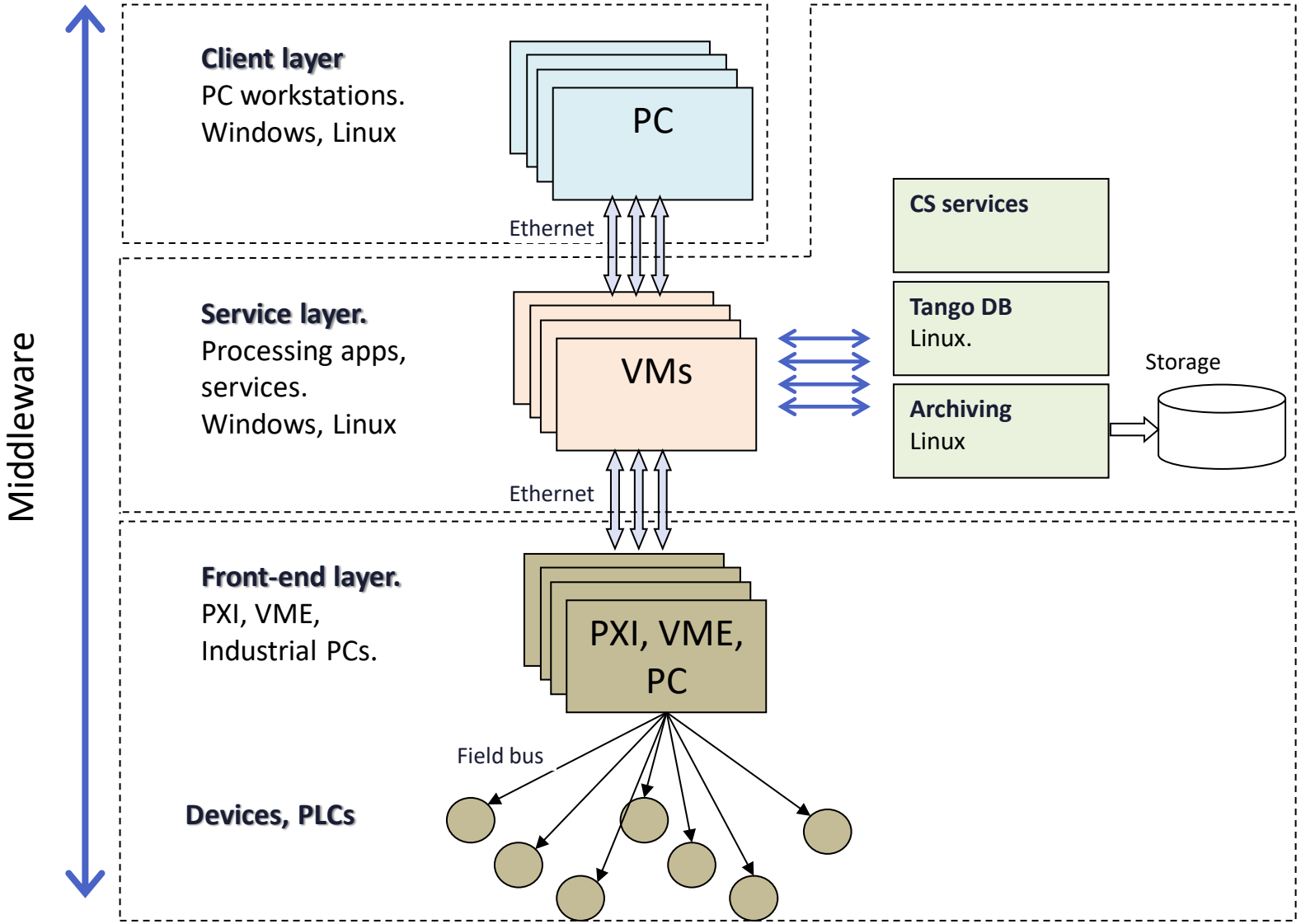
Stage III: Polarized Beams’ Mode of The Collider

- Spin Physics Detector (SPD)

Control System development goals

- Centralized control of heterogeneous distributed equipment
- Reliable operation and fast recovery
- Safe operation, access restrictions
- Easy support, modification and scalability
- Fast development and deployment
- Easy integration of third-party systems

Control System layout



Middleware: TANGO controls

- CORBA based distributed object-oriented control system framework
- Multiplatform
- Hides network location and technical details
- Provides unified interface for hardware equipment or service:
  - Commands
  - Attributes
  - Properties
- Has services and tools for control implementation.

Frontend layer

Few possible variants to implement DAQ or control:

- Custom hardware
- Commercial off-the-shelf (COTS)

Primary requirements:

- Ease of development
- Quality, reliability and performance
- Maintenance of equipment during the accelerator complex life-time

Frontend layer




National Instruments PXI– high performance Eurocard packaging modular platform for measurements and automation systems:

- PCI express and PCI busses with additional synchronization buses.
- Excellent performance: PXIe-1085 – throughput up to 4GB/s per slot and up to 12GB/s per system.
- Wide range of available modules (1500+) – controllers, acquisition boards, analog and digital I/O, signal generators, digital multimeters, counters and timers, high speed digitizers, industrial interfaces, RF and others.
- Windows and Linux programming – LabVIEW, C++ and C# libraries.
- Excellent support.

Frontend layer

- Digital signal processing (DSP) modules FlexRIO –PXI and PXIe modules with Xilinx FPGA and custom I/O modules. Supports peer-to-peer streaming up to 3GB/s.
- Compact RIO - High performance embedded systems and intellectual controllers based on Xilinx FPGA + ARM with standard or custom I/O module.

Frontend layer

Tango drivers with runtime configurable properties for NI equipment were developed:

- Digitizers and scopes
- Analog and digital I/O
- Timers and counters
- Digital multimeters
- RTD input modules
- TANGO interface for FlexRIO and CompactRIO.

Combination of tango devices can be used to quickly deploy a solution based on almost any NI acquisition equipment.

Client layer

Possible variants:

- usual GUI desktop applications – (QTango, Taurus, TangoATK)
- Web applications

Web-based applications advantages:

- Works on any platform (PC, mobile) and OS.
- Easier development – one application for all platforms.
- Easier maintenance: no need to install on PCs, centralized updates.

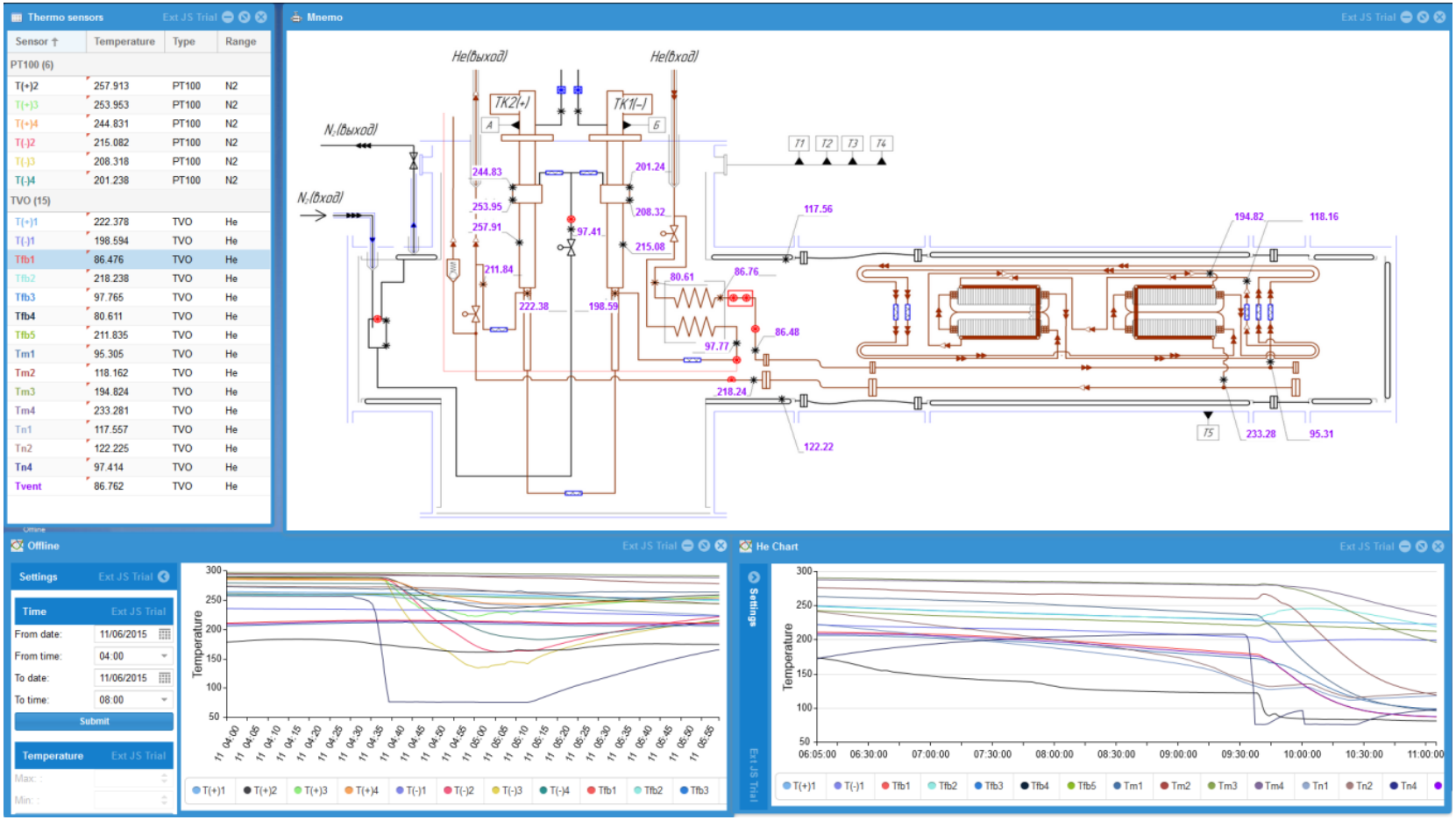
Client layer: Web apps

Communication between TANGO and Web application is required.

- RestDS – Tango module to provide access to TANGO control system devices via http requests (GET, POST).
- WebSocketDS – Tango module to read TANGO devices attributes via WebSocket protocol: data can be “pushed” to the browser in realtime on demand.

Client layer: Web apps

ExtJS framework (JavaScript). Web-application developed as a web desktop: a number of widgets(tasks) with dynamic layout.



Service layer

Contain high-level TANGO device servers, representing whole subsystem:

- Collects and process data from low-level devices.
- Performs control loop.
- Provides standard interface to client applications: commands, attributes.

Service layer: Virtualization

Applications running on service layer are hardware independent and can be virtualized (run on VM):

- Easier management – fast VM deployment from templates, cloning, backups.
- Better tasks isolation – assign VM per task or group of tasks.
- Resources tuning – can assign appropriate CPU cores, disk space, RAM size, disk I/O.
- Resource utilization – efficient usage of host's RAM and CPU.
- High Availability - restore VM from failed server.

Proxmox VE - complete open source virtualization management solution for servers. It manages virtual machines, storage, virtualized networks, HA clustering and supports both:

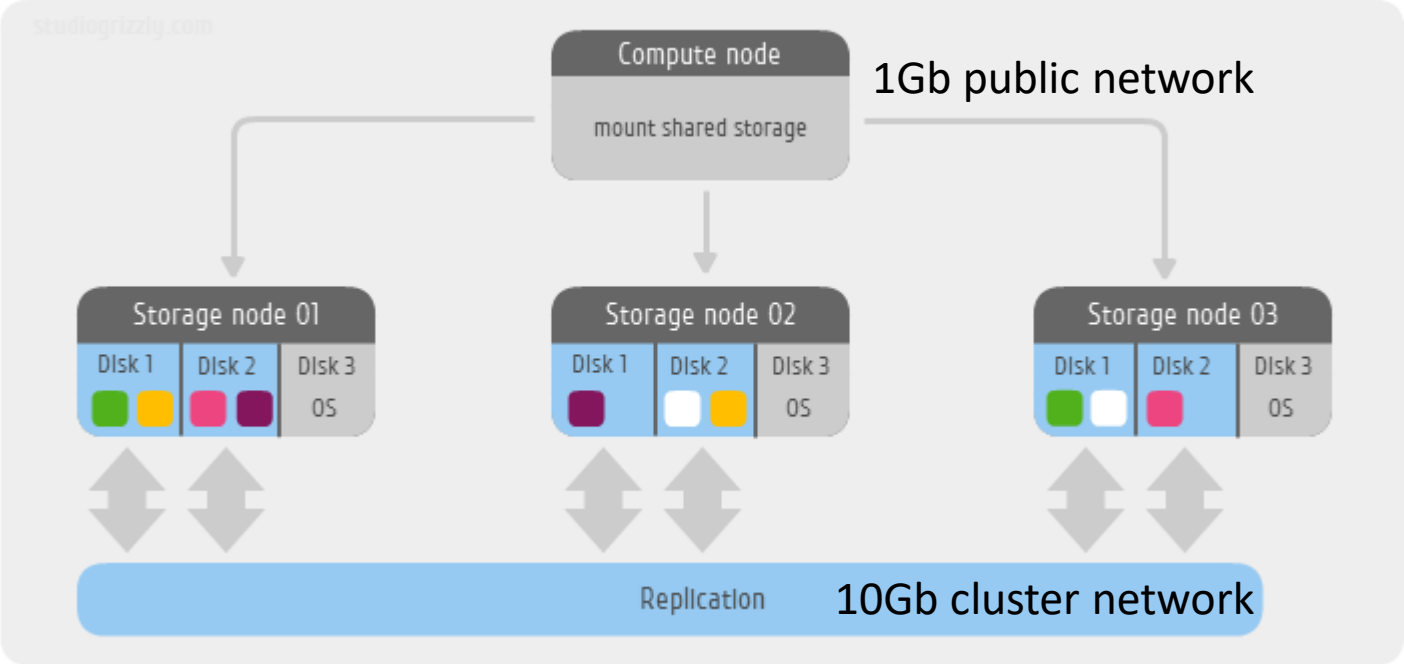
- **Kernel-based Virtual Machine (KVM)**
- **Container-based virtualization**

Service layer: Shared storage

- Crucial component of virtualization to provide high availability of VMs
- Need good performance , both transfer rate and IOPS to manage read/write operations of number of VM images
- Have to be redundant to provide data consistency in case of hardware or network failure
- Need to be scalable – should be able to add more storage space without loosing performance

CEPH storage

ceph is a distributed object store and file system. Ceph is highly reliable, easy to manage and open-source. It provides redundancy, excellent performance and scalability. Ceph storage cluster consists of large number of nodes which communicate with each other to distribute and replicate data dynamically.



Scalability

The scalability can be achieved by adding nodes to cluster. CEPH retains most characteristics at scale or even improves. Adding more nodes to run more VMs:

- Capacity increases
- Throughput increases
- IOPS increase
- CPU cores and RAM increase

Temporary impact during re-balancing.

High availability

We need to provide high availability of Tango services and fast failover in case of hardware problems.

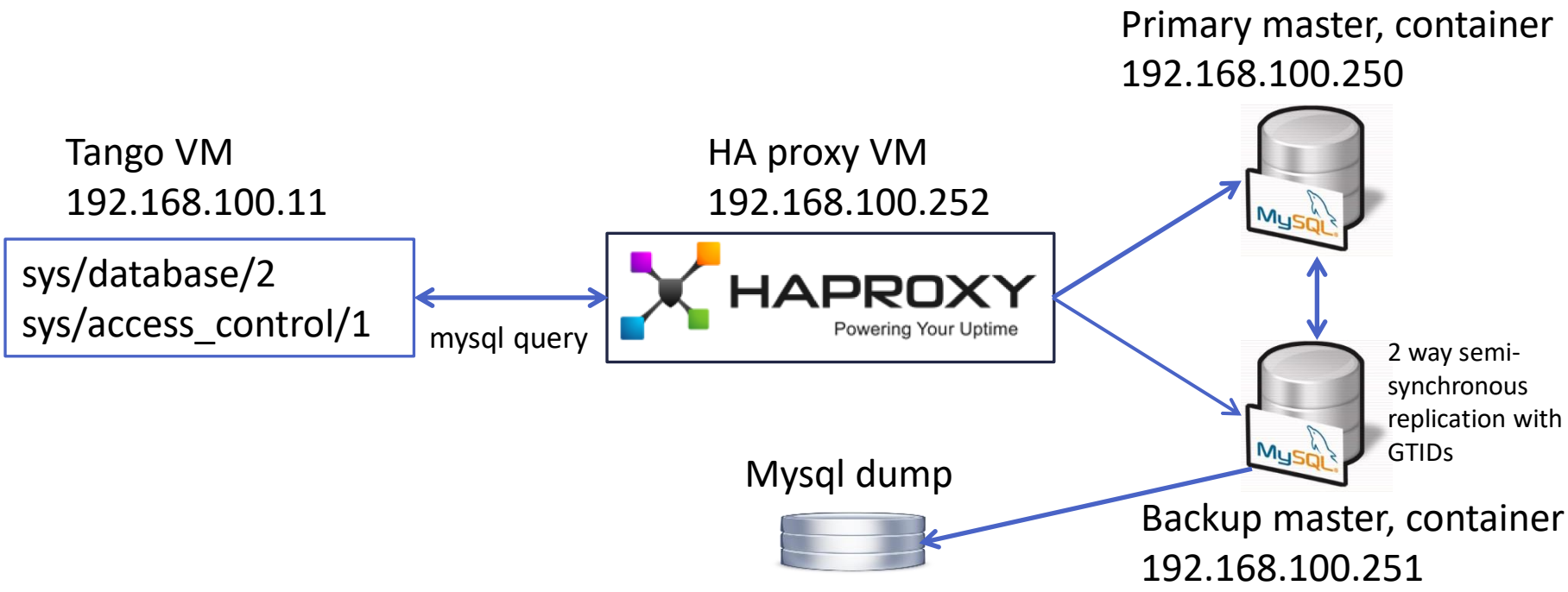
Hardware measures (UPS devices controlled by Network UPS tools, reliable enterprise class hard drives) + data redundancy (RAID, replication) + backups (VMs and databases):

- Virtual machines are running on Proxmox VE cluster with VM images stored on CEPH storage (replication=3). Any VM can be started on any node.
- TANGO database: vital for all other Control System Tango devices, running in Linux container on local storage for performance reasons.

High availability: TANGO DB

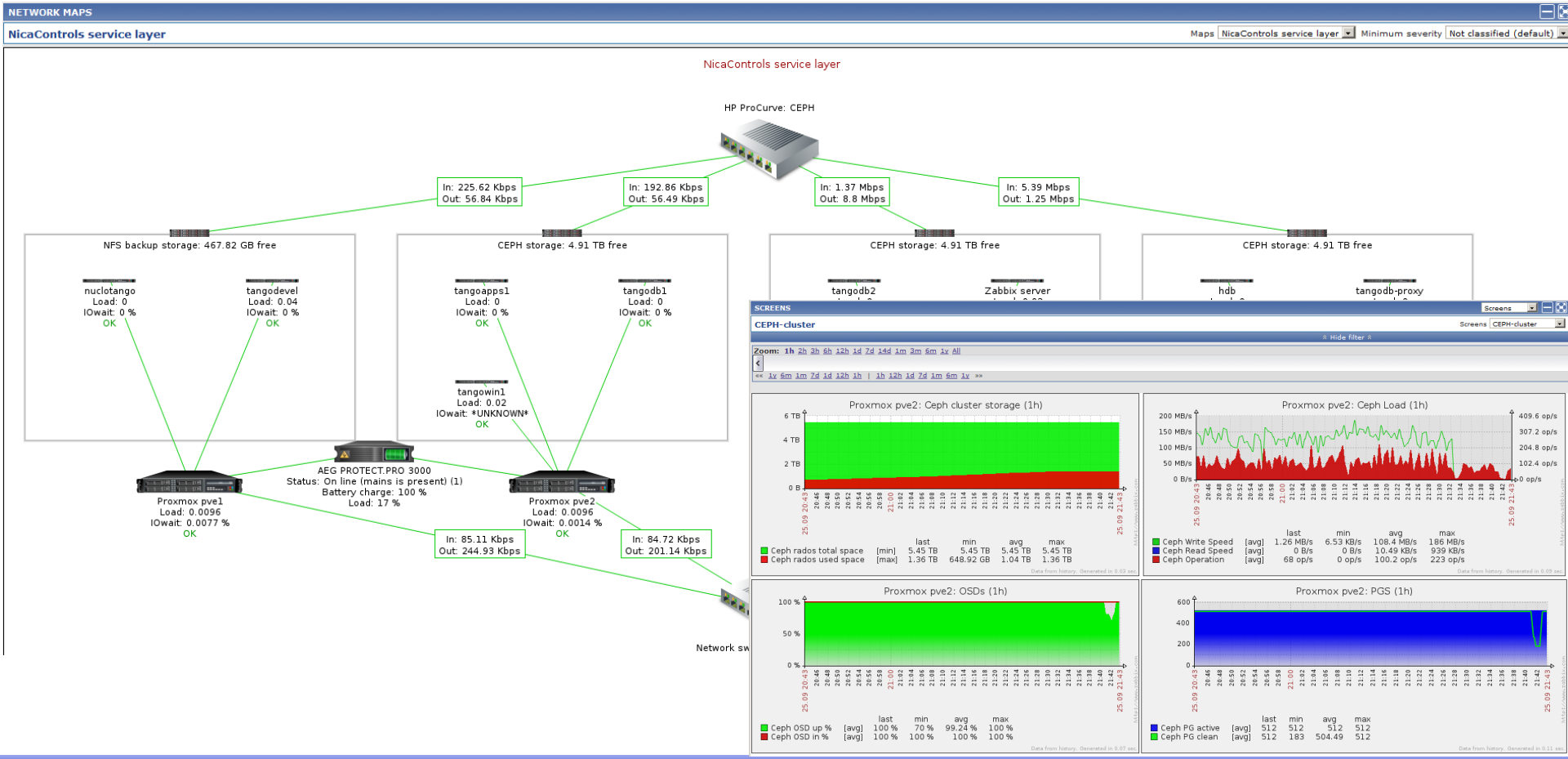
High Availability for Tango database can be achieved:

- Master-Master replication in active-passive mode.
- Load balancing and backup via HAPROXY



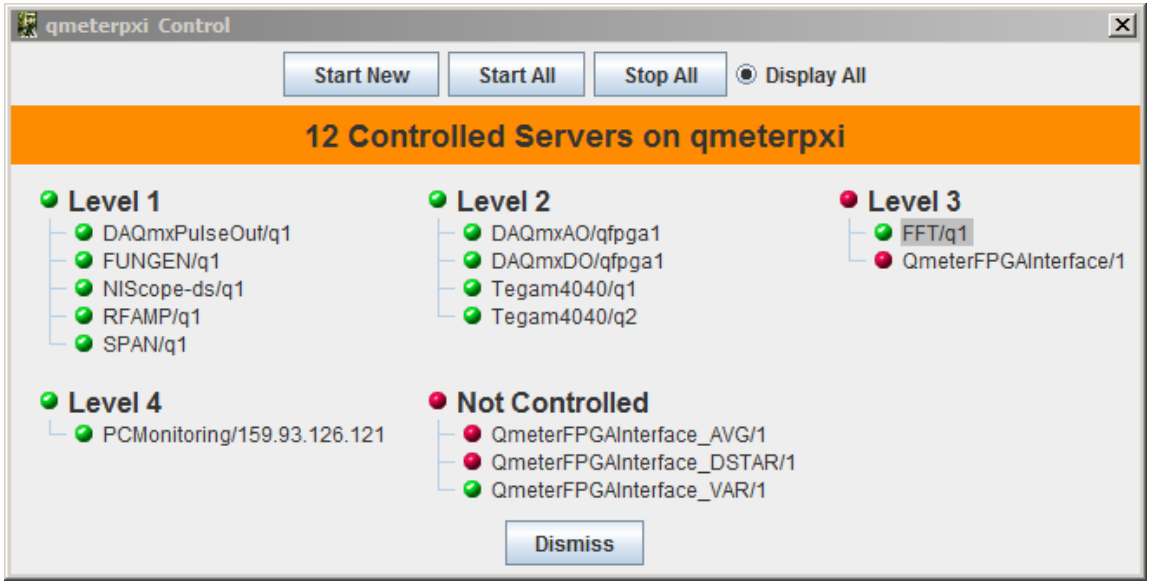
Hardware and software monitoring

Zabbix – monitoring hardware and software of Control System cluster: power, fans, CPU, RAM, disk space, network traffic, disk I/O, CEPH health and many other items. Alerts and notifications are sent via e-mail to cluster admins.



TANGO devices monitoring

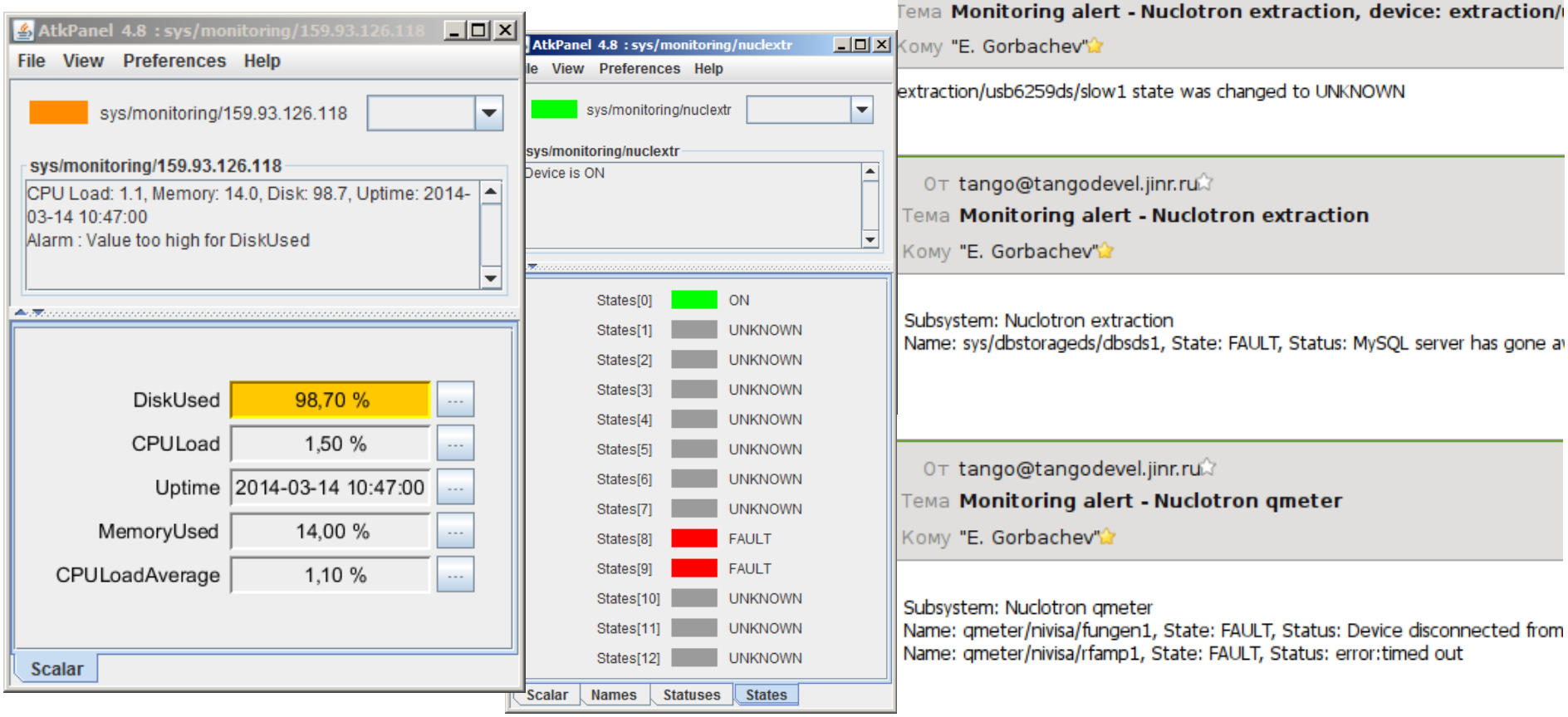
Astor/Starter –tools for remote control and monitoring of TANGO applications



Hosts	Servers
• All controlled servers are running. • Starter is starting server(s). • At least, one controlled server is stopped. • Starter is not running on host.	• Server is running • Server is running but not alive (Starting ?) • Server is not running.

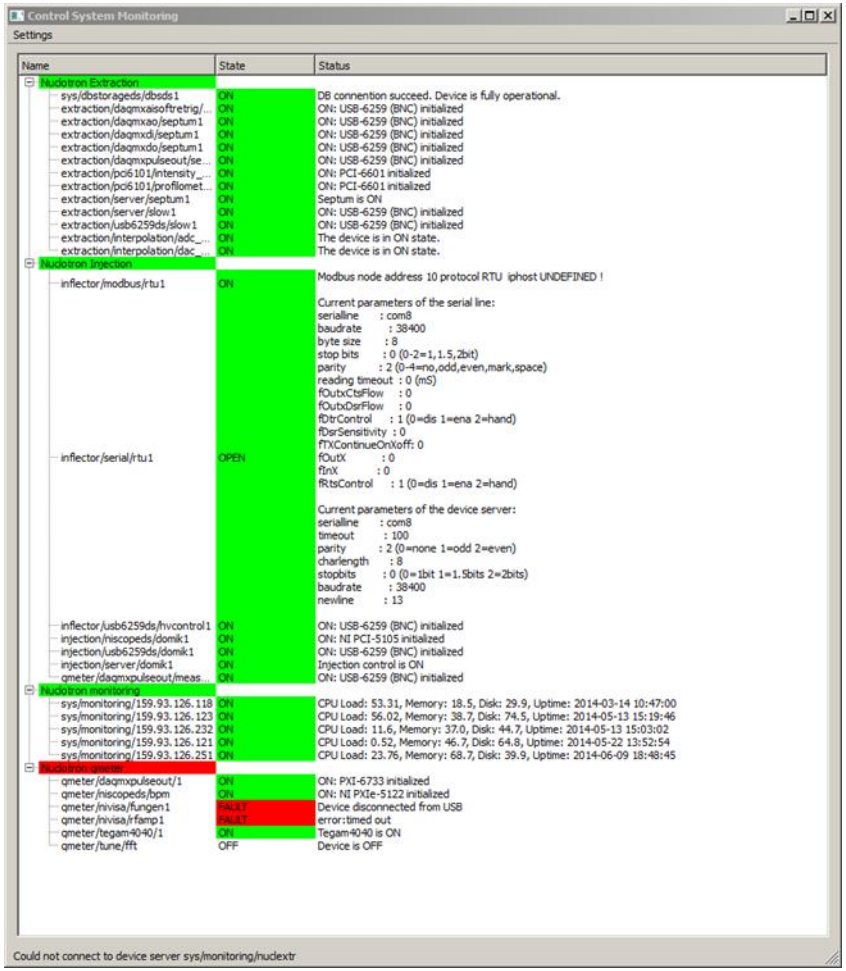
TANGO devices monitoring

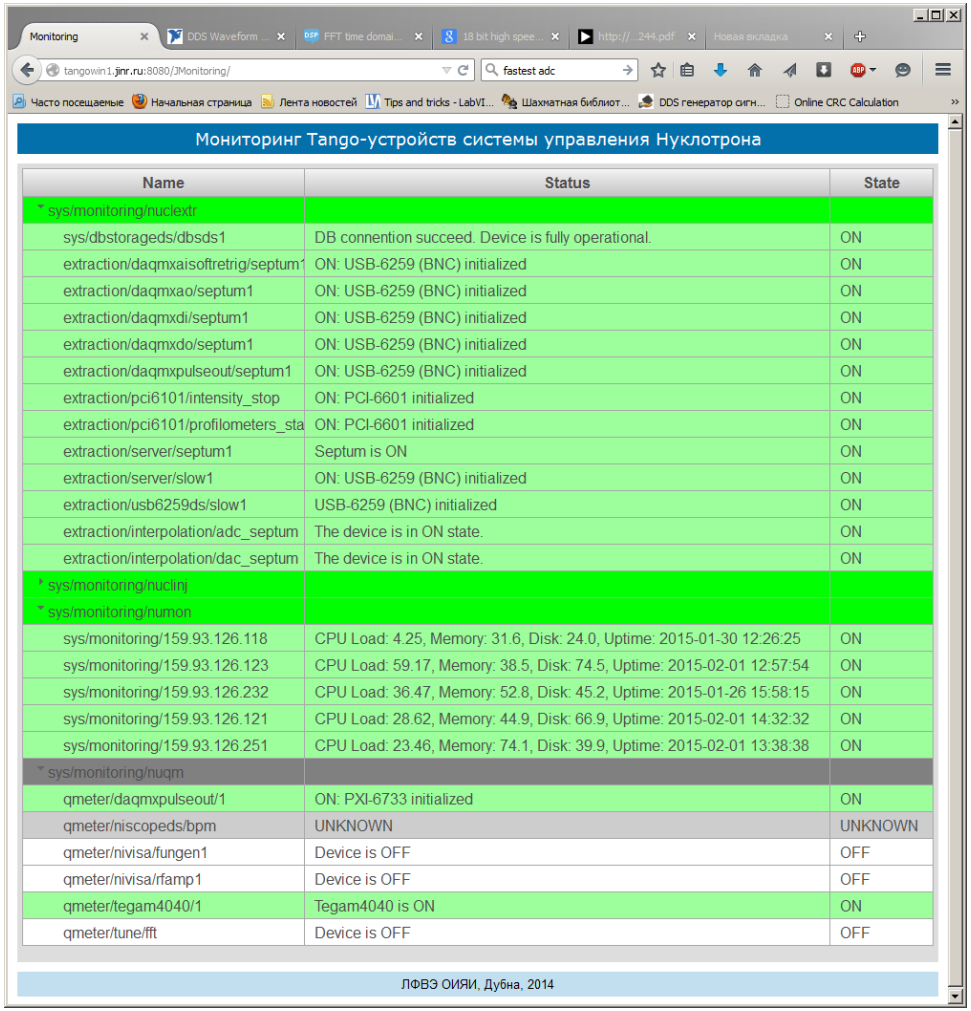
Special TANGO services to check frontend computers resources and states of TANGO devices. Alerts and notifications are sent via e-mail to tango admins.



TANGO devices monitoring

Desktop and web clients to represent states and statuses of TANGO



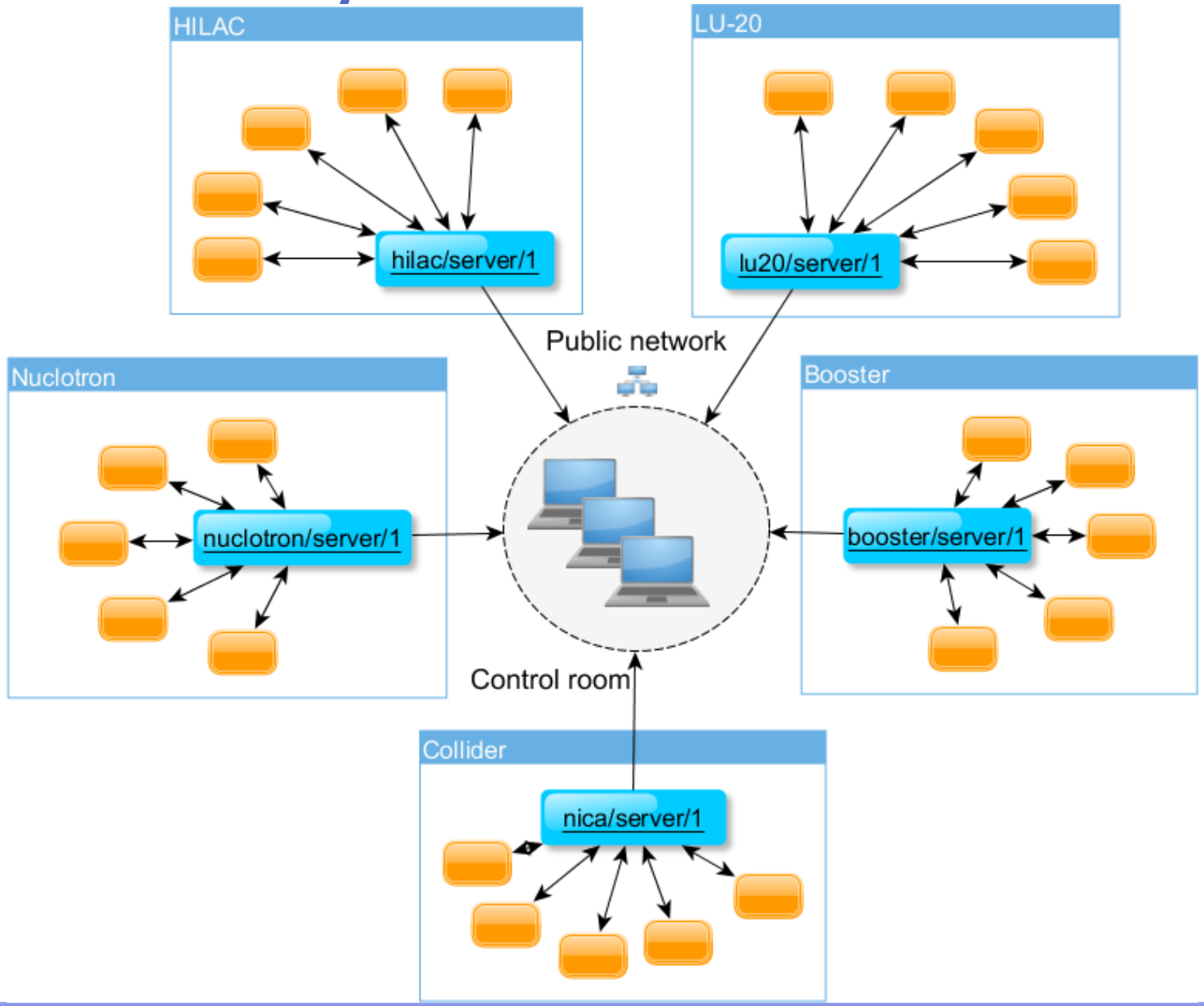


Access control

Access control and security are vital to safely run a distributed control system**.**

1) **Network** configuration:
   - Firewall configuration to provide access for certain IP range.
     - Complex list of rules, fixed ports to run device servers
   - Private sub networks for accelerators control systems with restricted access.
     - Need to provide limited access from external networks

Control system communications

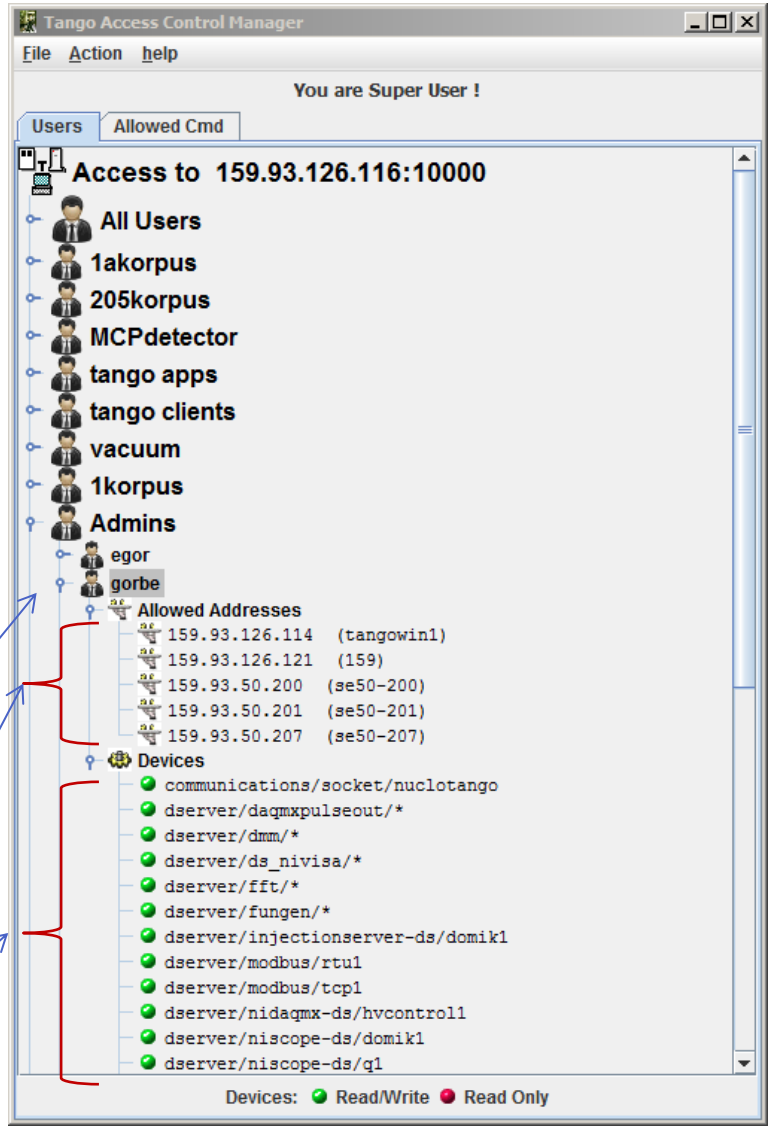


Access control

2) **Software security** checks:
   - Ask for username/password on client side to execute certain operations:
     - Can not prevent execution by other clients (jive)
   - Checks clients rights on server side:
     - Have to distinguish clients and store information about their rights.

Access control

3) **Tango client-side** access control
   - Optional service restricting devices commands execution and attributes writes based on client username & IP checks.
     - Not flexible
   - Applies on Tango::DeviceProxy creation.
     - Need client restart
     - Not applicable for web clients.



Access control

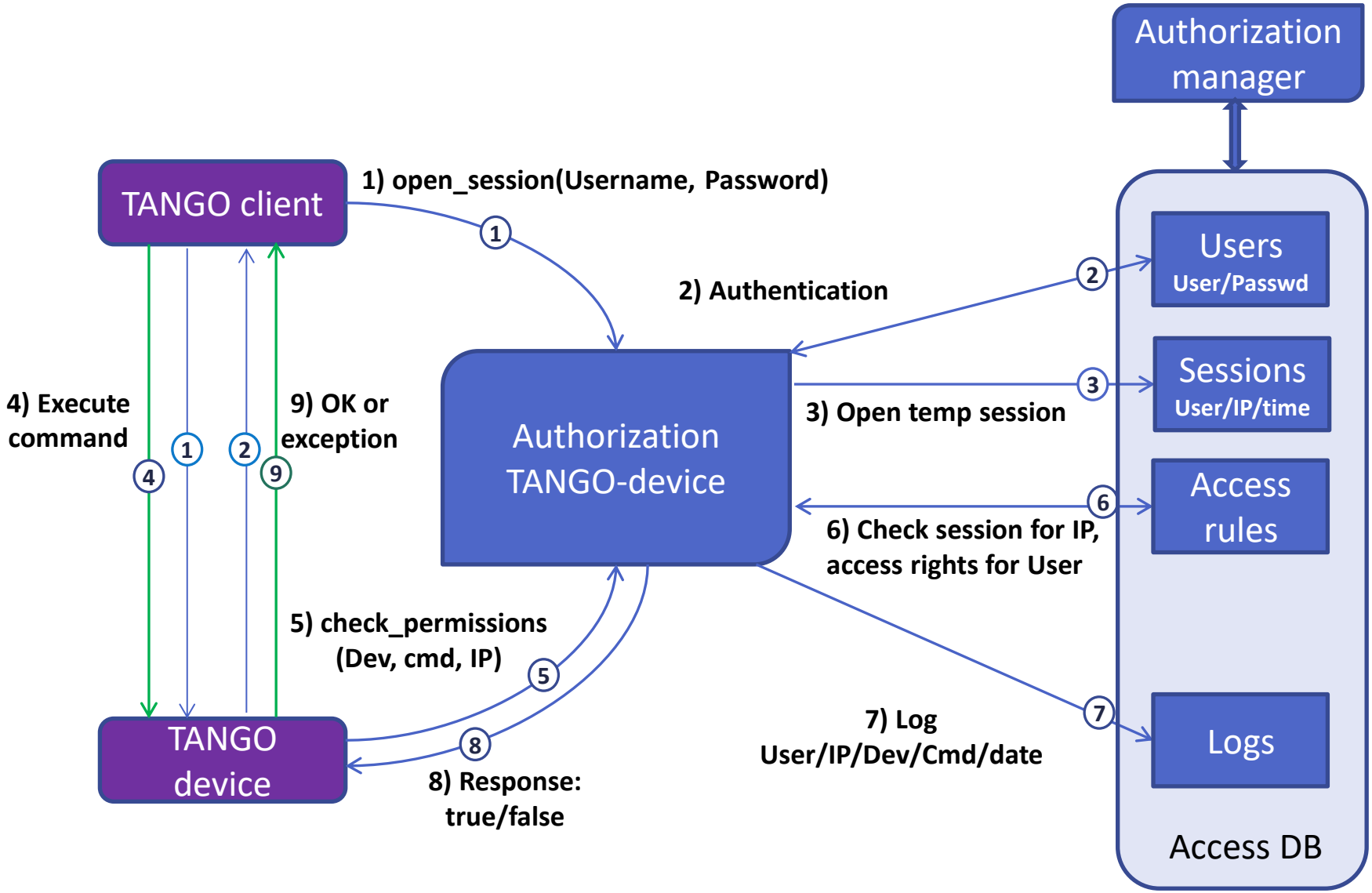
Idea:

- Improve access control by **additional** server side security checks

Goals:

- Centralized management of user's permissions
- Centralized access logs
- No complications to both Tango device server and client development
- No modifications to Tango library

Access control

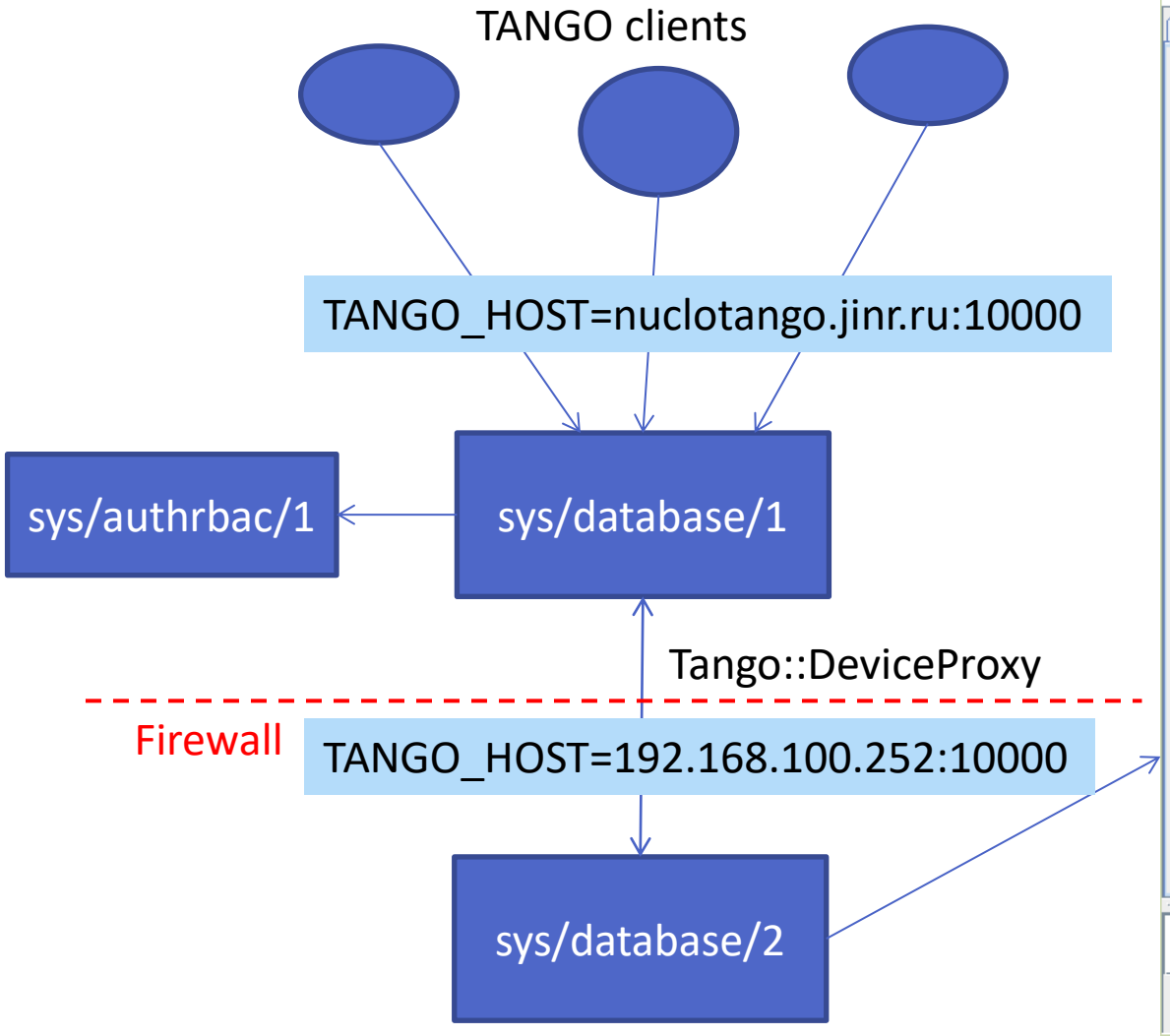


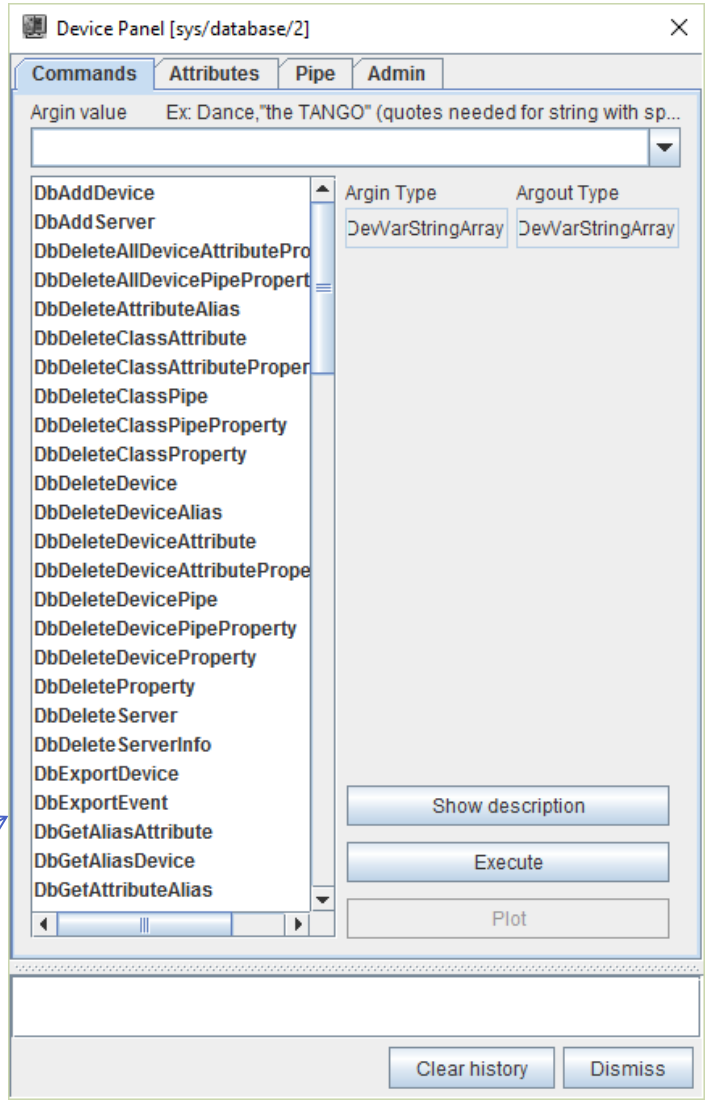
Access control

Realization details:

1. Role Based Access Control (RBAC).
   - Each role have a group of permissions.
   - Several roles can be assigned to user/IP pair
   - priorities
2. Authentication by location (IP address) .
   - Access from operator's PC and CS core servers without passwords.
3. Support of MySQL regular or wildcard expressions in rules and addresses: can be configured as Tango property.
4. Objects access cache for improving performance.
5. Centralized logging service for TANGO devices.
6. Providing simple interface for TANGO devices to check client's permissions and to log information in the central database.

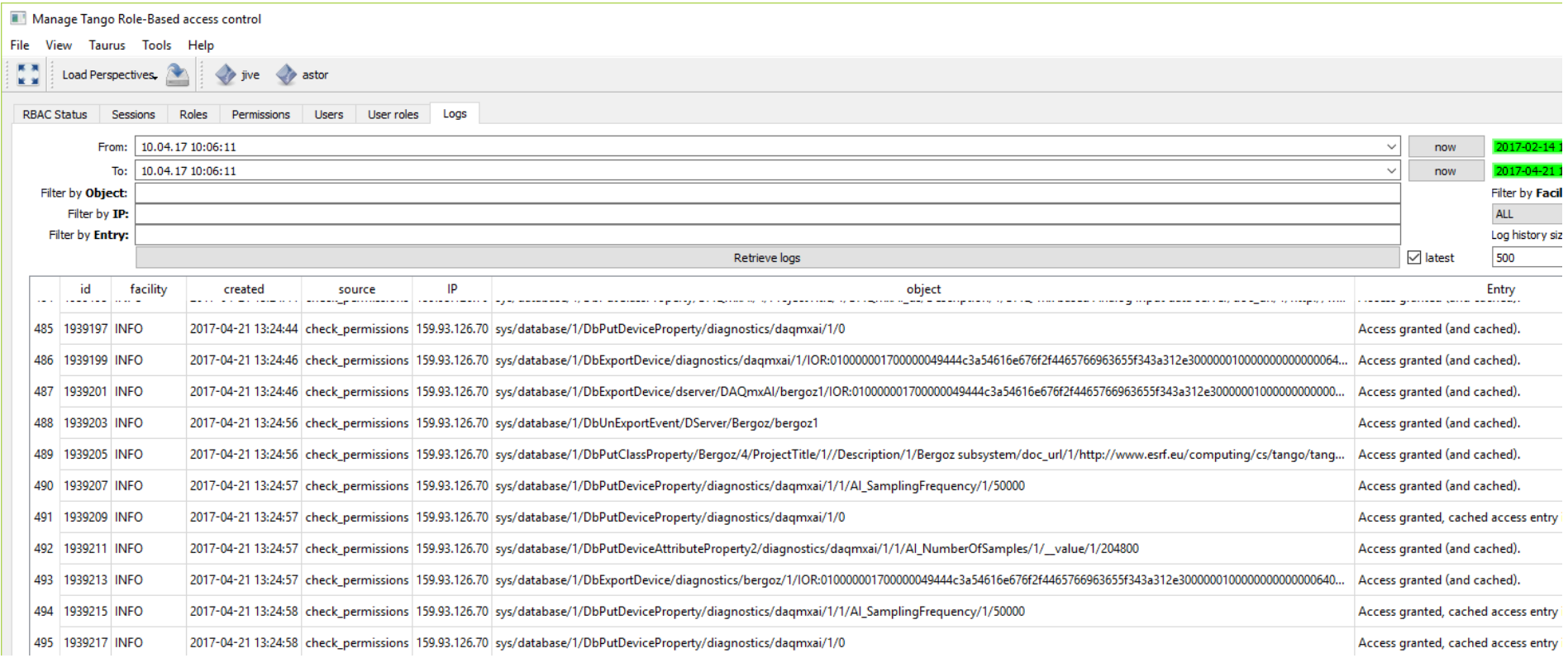
TANGO database protection





Logging

- Full logs of TANGO database changes – exporting devices, changing properties etc.
- Provide easy way for TANGO devices centralized logging command execution, attributes changes and other important information.
- Flexible interface for administrators to find information in logs.



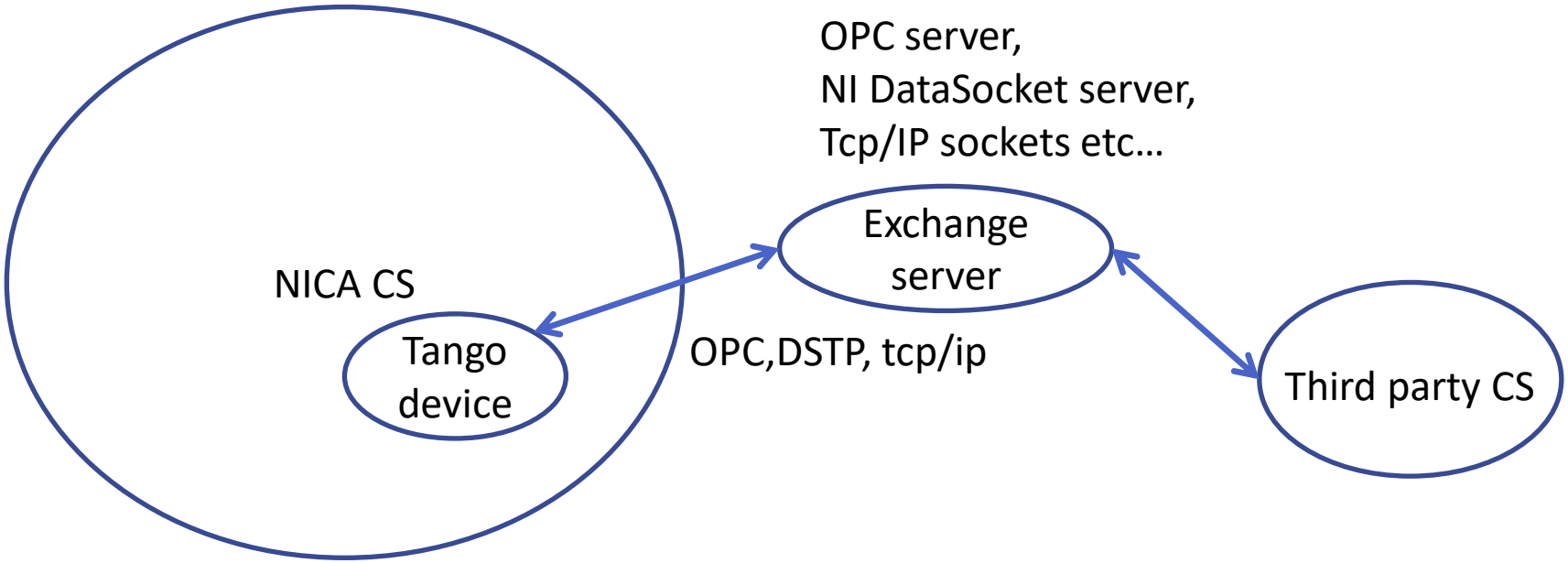
	id	facility	created	source	IP	object	Entry
485	1939197	INFO	2017-04-21 13:24:44	check_permissions	159.93.126.70	sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/0	Access granted (and cached).
486	1939199	INFO	2017-04-21 13:24:46	check_permissions	159.93.126.70	sys/database/1/DbExportDevice/diagnostics/daqmxai/1/IOR:010000001700000049444c3a54616e676f2f4465766963655f343a312e3000000100000000000000064...	Access granted (and cached).
487	1939201	INFO	2017-04-21 13:24:46	check_permissions	159.93.126.70	sys/database/1/DbExportDevice/dserver/DAQmxAI/bergoz1/IOR:010000001700000049444c3a54616e676f2f4465766963655f343a312e3000000100000000000...	Access granted (and cached).
488	1939203	INFO	2017-04-21 13:24:56	check_permissions	159.93.126.70	sys/database/1/DbUnExportEvent/DServer/Bergoz/bergoz1	Access granted (and cached).
489	1939205	INFO	2017-04-21 13:24:56	check_permissions	159.93.126.70	sys/database/1/DbPutClassProperty/Bergoz/4/ProjectTitle/1//Description/1/Bergoz subsystem/doc_url/1/http://www.esrf.eu/computing/cs/tango/tang...	Access granted (and cached).
490	1939207	INFO	2017-04-21 13:24:57	check_permissions	159.93.126.70	sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/1/AI_SamplingFrequency/1/50000	Access granted (and cached).
491	1939209	INFO	2017-04-21 13:24:57	check_permissions	159.93.126.70	sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/0	Access granted, cached access entry
492	1939211	INFO	2017-04-21 13:24:57	check_permissions	159.93.126.70	sys/database/1/DbPutDeviceAttributeProperty2/diagnostics/daqmxai/1/1/AI_NumberOfSamples/1/__value/1/204800	Access granted (and cached).
493	1939213	INFO	2017-04-21 13:24:57	check_permissions	159.93.126.70	sys/database/1/DbExportDevice/diagnostics/bergoz/1/IOR:010000001700000049444c3a54616e676f2f4465766963655f343a312e3000000100000000000000640...	Access granted (and cached).
494	1939215	INFO	2017-04-21 13:24:58	check_permissions	159.93.126.70	sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/1/AI_SamplingFrequency/1/50000	Access granted, cached access entry
495	1939217	INFO	2017-04-21 13:24:58	check_permissions	159.93.126.70	sys/database/1/DbPutDeviceProperty/diagnostics/daqmxai/1/0	Access granted, cached access entry

Data archiving

HDB++ archiving system:

- Store TANGO attributes values into a database (SQL or noSQL).
- Publish/subscribe paradigm via TANGO archiving events – storing only valuable information.
- Highly scalable - multiple archivers to distribute load over few servers and disk storages.
- Under tests now on Superconducting Magnets Test Bench – storing about 500 TANGO attributes
- JINR data archiving configuration GUI and extractor GUI – to be developed.

Integration of third-party systems



Tango device to provide interface to external control system and represent it to NICACS:

- OPC (vacuum, cryocooler)
- NI DataSocket (Electron cooling)
- TCP/IP socket (Booster RF)

Conclusions

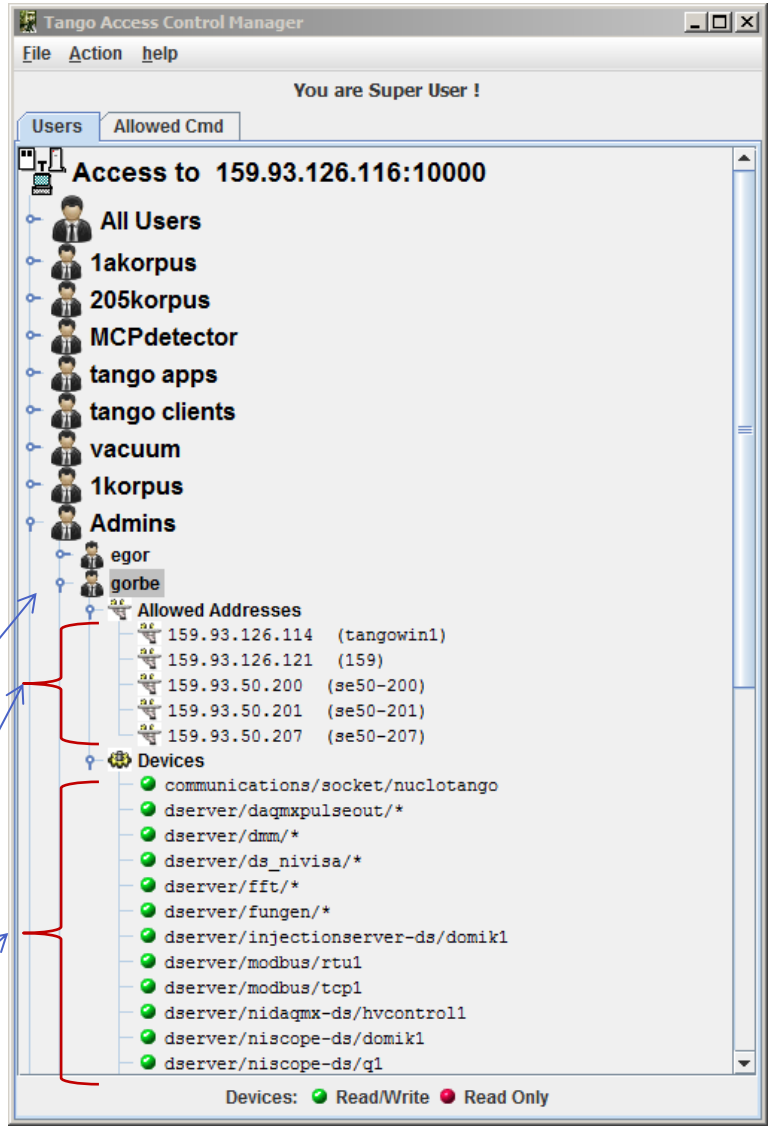
Distributed, scalable control system infrastructure based on Tango has been developed to provide fast development, deployment and safe execution:

code generation, TANGO drivers for NI equipment, deployment on dedicated VM in HA cluster, server-based access control, hardware and software monitoring, data archiving, equipment and software database.

Thank you for your attention!

Service layer: Access control

3) **Tango client-side** access control
   - Optional service restricting devices commands execution and attributes writes based on client username & IP checks.
     - Not flexible, easy to pass.
   - Applies on Tango::DeviceProxy creation.
     - Need client restart



Service layer: Access control

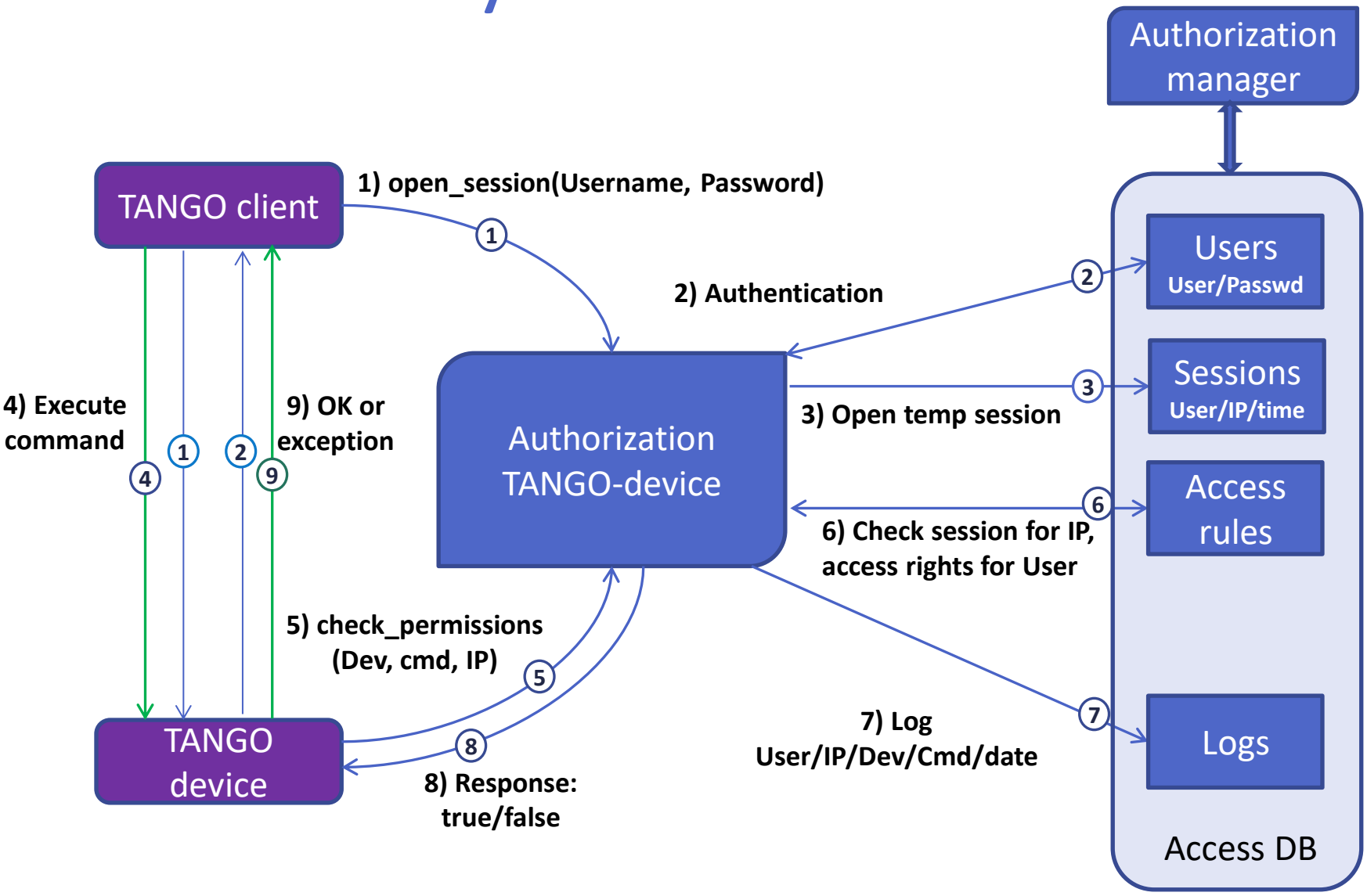
Idea:

- Improve access control by **additional** server side security checks

Goals:

- Centralized management of user's permissions
- Centralized access logs
- No complications to both Tango device server and client development
- No modifications to Tango library

Service layer: Access control



Service layer: Access control

Realization details:

1. Role Based Access Control (RBAC).
   - Each role have a group of permissions.
   - Few roles can be assigned to user/IP pair
2. Authentication by location (IP address).
   - Default Operator role and user
   - Operator user has no password
3. Support of MySQL regular or wildcard expressions in rules and addresses: can be configured as Tango property.
4. Objects access cache for improving performance.

Service layer: RBAC

	uid	login	last name	first name	phone	email	password	enabled
0	1	operator	NULL	NULL	NULL	NULL	!	1
1	2	gorbe	Gorbachev	Evgeny	63057	egorbe@gmail.com	{MD5}cacbcc3edf3f5f46179588bdd974ffe2	1
2	3	egor	Sedykh	Georgy		egor@dubna.tk	{MD5}9990775155c3518a0d7917f7780b24aa	1

	user_role_id	user_id	role_id	ipaddr_expr
2	3	1:operator	2:rbac-admin	127.0.0.1
3	4	1:operator	2:rbac-admin	159.93.50.200
4	5	1:operator	2:rbac-admin	159.93.50.207
5	9	1:operator	3:export-device	159.93.50.200
6	13	1:operator	3:export-device	159.93.50.176
7	19	1:operator	3:export-device	159.93.50.207
8	11	1:operator	4:put-property	159.93.50.200

	role_id	role_name	descripion	enabled
0	1	operator	operator permissions	1
1	2	rbac-admin	RBAC authorization management	1
2	3	export-device	export a tango device	1
3	4	put-property	add/delete a tango property	1

Service layer: RBAC

	permission_id	role_id	object_expr	priority	enabled
0	3	1:operator	sys/database/1/DbInfo	10	1
1	2	1:operator	sys/database/1/DbImport%	10	1
2	1	1:operator	sys/database/1/DbGet%	10	1
3	5	2:rbac-admin	sys/managerbac/1/%	0	1
4	4	2:rbac-admin	sys/authrbac/1/%	0	1
5	39	3:export-device	sys/database/1/DbDeleteAll%	10	1
6	33	3:export-device	sys/database/1/DbUnExportServer/%	10	1
7	29	3:export-device			
8	27	3:export-device			
9	25	3:export-device			
10	23	3:export-device			
11	31	4:put-property			

	role_id	role_name	descripion	enabled
0	1	operator	operator permissions	1
1	2	rbac-admin	RBAC authorization management	1
2	3	export-device	export a tango device	1
3	4	put-property	add/delete a tango property	1
4	5	authtest	use TagoAuthTest commands	1
5	9	add-device	add a new tango device	1
6	11	tango-admin	using astor/logviewer	1
7	13	tomography	using diagnostics/tomography	1

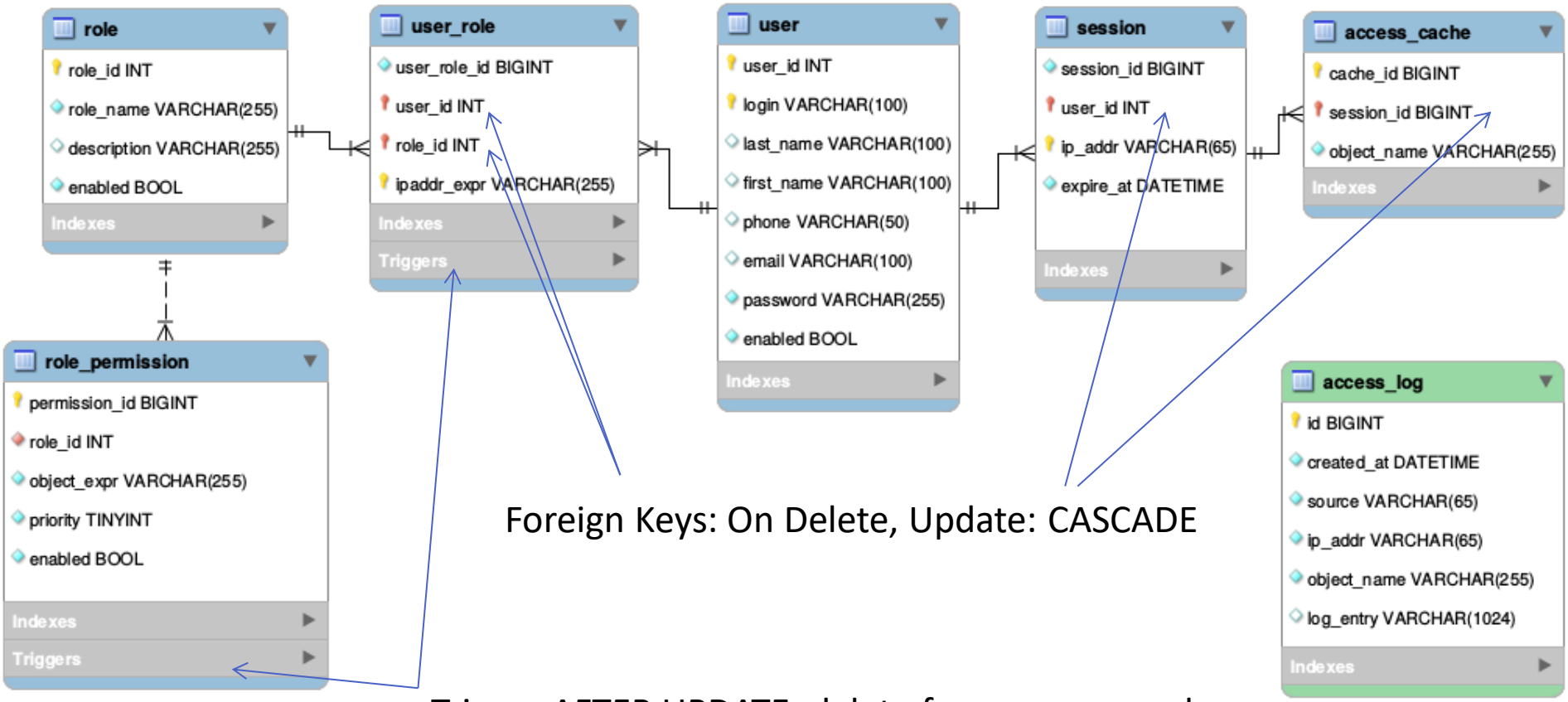
Service layer: Access logs

	id	created	source	IP	object	Entry
8	17	2016-06-21 14:50:06	open_session	159.93.50.207	gorbe	Session opened.
9	19	2016-06-21 14:50:11	authenticate	159.93.50.207	gorbe	Authentication successful.
10	21	2016-06-21 14:50:11	close_session	159.93.50.207	gorbe	Session closed
11	23	2016-06-21 14:50:24	authenticate	159.93.50.207	gorbe	Authentication failure - wrong password.
12	25	2016-06-21 14:50:30	authenticate	159.93.50.207	gorbre	Authentication failure - user unknown.
93	187	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/name,exported,version,ior,ser...	Access granted (and cached).
94	189	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/name,exported,version,ior,ser...	Access granted (and cached).
95	191	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/device,value FROM property_d...	Access granted (and cached).
96	193	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/device,value FROM property_d...	Access granted (and cached).
97	195	2016-06-23 13:43:44	check_permissions	159.93.50.207	sys/database/1/DbMySqlSelect/device,value FROM property_d...	Access granted (and cached).
98	197	2016-06-23 13:45:20	check_permissions	159.93.50.207	sys/database/1/DbAddDevice/LogConsumer/se50-207@68	Access granted (and cached).
99	199	2016-06-23 13:45:20	check_permissions	159.93.50.207	sys/database/1/DbExportDevice/dserver/LogConsumer/se50-...	Access granted (and cached).
100	201	2016-06-23 13:45:20	check_permissions	159.93.50.207	sys/database/1/DbExportDevice/tmp/log/se50-207@68	Access granted (and cached).
109	219	2016-06-23 16:41:40	check_permissions	159.93.50.207	sys/database/1/DbAddDevice/NIScopeSaver/1	Access granted (and cached).
110	221	2016-06-23 16:41:58	check_permissions	159.93.50.207	sys/database/1/DbUnExportEvent/DServer/NIScopeSaver/1	Access granted (and cached).
111	223	2016-06-23 16:41:58	check_permissions	159.93.50.207	sys/database/1/DbPutClassProperty/NIScopeSaver	Access granted (and cached).
112	225	2016-06-23 16:41:58	check_permissions	159.93.50.207	sys/database/1/DbExportDevice/dserver/NIScopeSaver/1	Access granted (and cached).
113	227	2016-06-23 16:41:58	check_permissions	159.93.50.207	sys/database/1/DbDeleteDeviceProperty/dserver/NIScopeSav...	Access granted (and cached).

Property:

skip_logging_for	sys/database/1/DbImportDevice sys/database/1/DbGet

Service layer: Access control



Foreign Keys: On Delete, Update: CASCADE

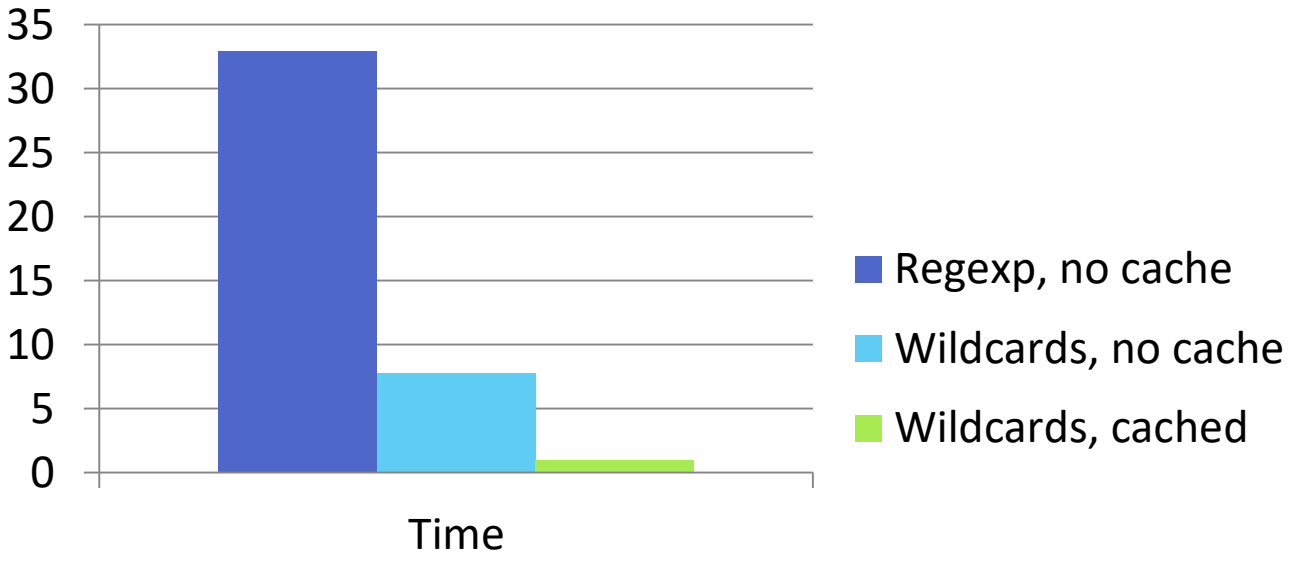
Trigger AFTER UPDATE: delete from access_cache;

Passwords are MD5 hashed

Access control performance

RBAC server performance tests, 10000 permissions checks, 1 thread

Test	Regexp, no cache	Wildcards, no cache	Wildcards, cached
Time per one permission check, ms	**32.95**	**7.79**	**0.95**



Service layer: Access control

Usage in TANGO device server:

1) Initialization:

```
#include "TangoAuth.h“
TangoAuthClientClass *auth;
```

In init_device():

```
auth=new TangoAuthClientClass(this);
```

In delete_device():

```
delete auth;
```

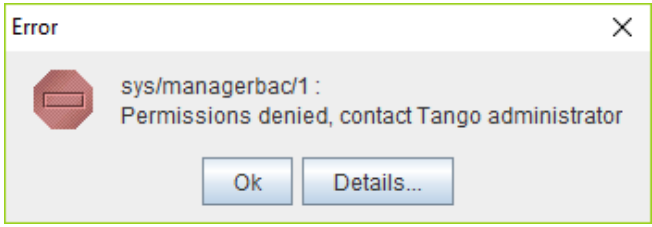
2) Usage:

In method cmd_name:

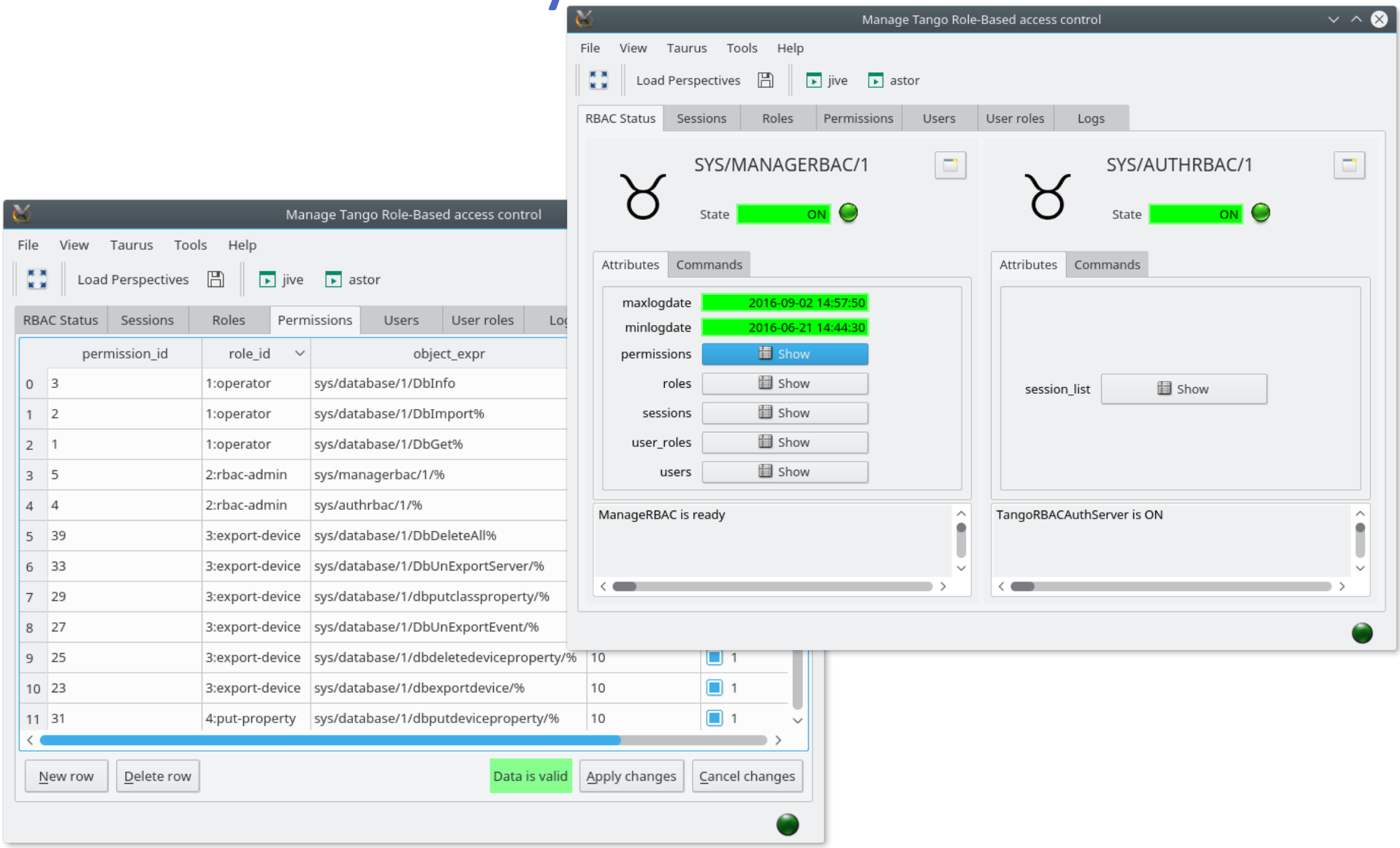
```
auth->CheckAccess(“cmd_name");
```

Or in always_executed_hook():

```
auth->CheckAccess(“any");
```



Service layer: Access control



Service layer: Access control

Protection of TANGO database:

Idea:

- Provide access to TANGO database with security checks and logging.

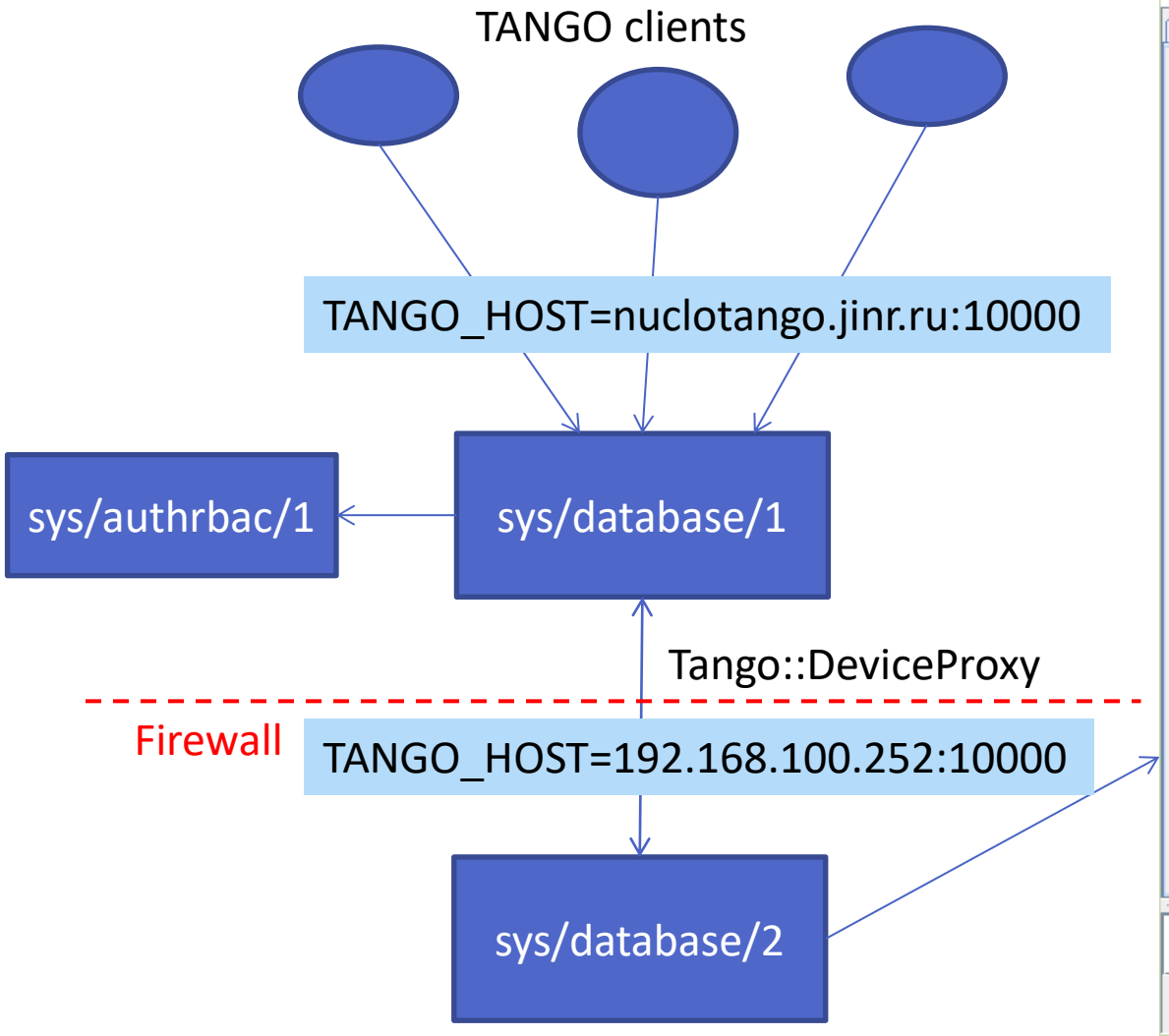
Possible solutions:

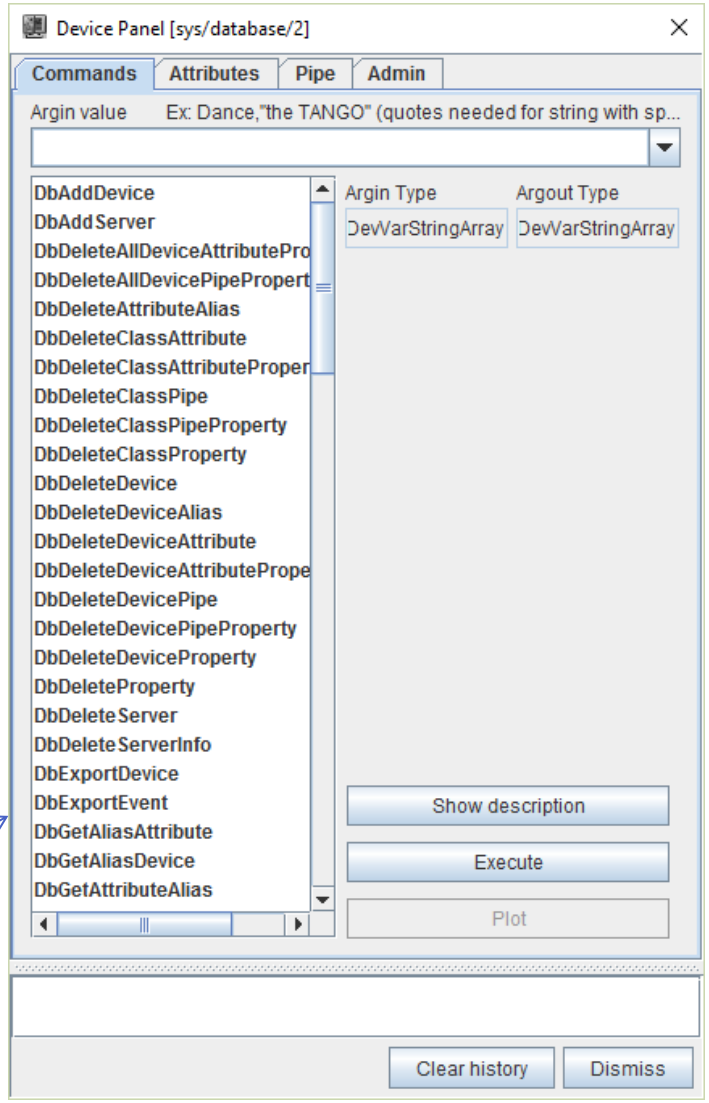
- Modification of each method of original Tango database server.
- Additional layer between clients and Tango database server.

Goals:

- Flexible rights separation – export device, add device, edit properties.
- Acceptable performance.

Service layer: Access control





Service layer: Access control

Realization:

1) Initialize

Tango::Util::_UseDb = false;

set_serial_model(Tango::NO_SYNC);

2) Create dynamic commands and attributes.

dbdev = new Tango::DeviceProxy("sys/database/2");

cmdlist=dbdev->get_command_list();

cmdinfo=dbdev->get_command_config(cmdlist);

3) All dynamic commands use the same command class with method execute():

- Check access with command name
- Execute command on original device with arguments
- Return result to client

Service layer: Access control

Database server performance tests:
4 parallel threads executing
time for i in `seq 1 1000`;do ./tango_exec sys/database/1 DbInfo > /dev/null; done

Database server	sys/database/2 (standard DB server)	sys/database/1 (with access control, cached)
Time per one command, ms	23.690	25.245

Global timing and synchronization

Timing and synchronization system is an important part of the accelerating complex:

- Global time reference for geographically distributed equipment.
- Beam diagnostics synchronization – closed orbit measurements.
- Beam transfer synchronization with different scenarios: bunch to bucket, barrier buckets.
- Events and signals distribution.

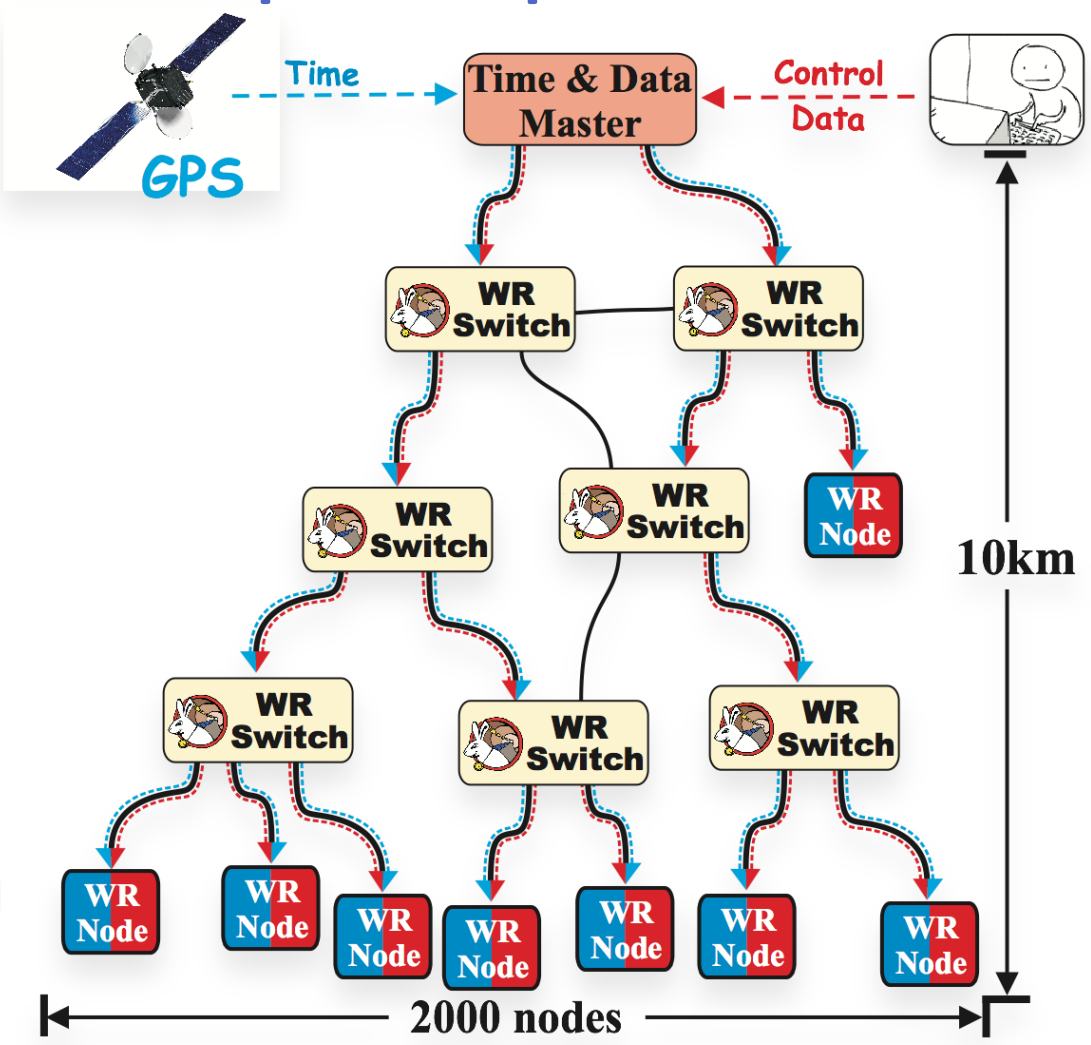
White Rabbit principles

Layout:

- Tree layout with synchronization master on the top.
- Single fiber optic for RX/TX

Features:

- sub-nanosecond synchronization
- connecting thousands of nodes
- typical distances of 10 km between nodes
- Ethernet-based gigabit rate reliable data transfer
- fully open hardware, firmware and software
- multi-vendor commercially produced hardware
- Based on IEEE-1588 (PTP)
- 1Gb/s transfer rate

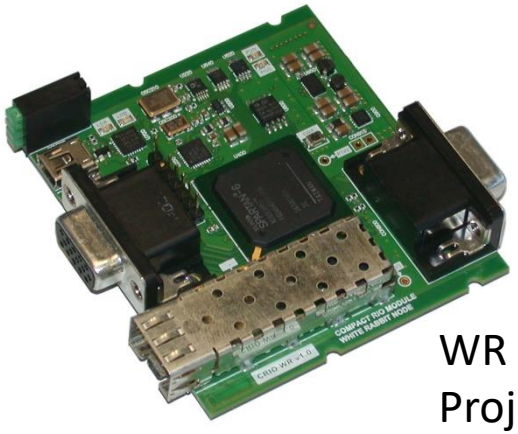


White Rabbit elements

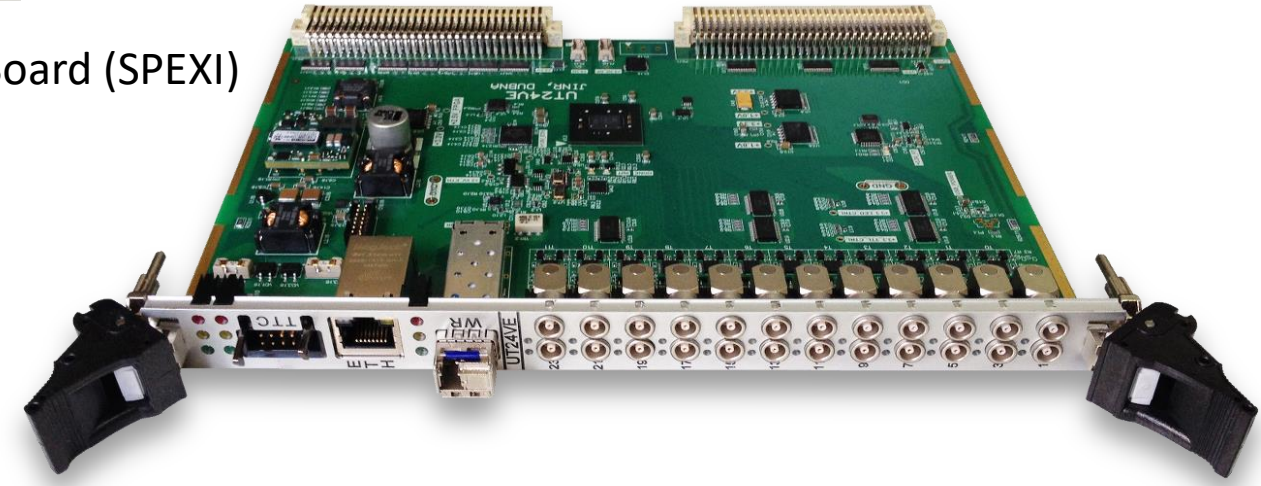
- Designated fiber optic network
- Endpoint devices with embedded *White Rabbit Protocol Core*
- WhiteRabbit switches *WRS-3/18*
- GPS/GLONASS Time receiver
- Rubidium frequency standard generator *Pendulum CNT-91R*

Modules with White Rabbit support

Simple PXI express FMC Carrier Board (SPEXI)
Project on www.ohwr.org



WR node in CompactRIO format.
Project on www.ohwr.org



UT24VE – universal input/output. Works on B@MN

NICA CS prototypes

- Booster thermo diagnostics – 320 channels NI PXIe based RTD measurements.
- Booster magnetic cycle control – FlexRIO + custom IO modules.
- Booster RF – integration of third-party CS.
- Booster/Linac vacuum – integration of third-party SCADA control.
- NICA injection/extraction control – CompactRIO + custom IO modules.
- Booster/NICA orbit correction.
- Beam diagnostics (profiles, intensity, tune measurements) – NI PXIe
- SC magnets test bench- thermometry (NI PXIe), satellite refrigerators control (interface to SCADA)
- WhiteRabbit on B@MN aquisition