JINR
DUBNA

Development of NICA Control System: Access Control and Logging

E. Gorbachev, G. Sedykh,   JINR, Dubna, Russia

NICA accelerator complex is under construction at JINR, Dubna. It will consists of heavy ion and polarized particle sources, RFQ injector, heavy- and light-ion linear accelerators, superconducting booster synchrotron, existing Nuclotron synchrotron and two superconducting collider rings (Fig. 1). Important dates:
2019: Stage I – Full injection complex + Booster + Nuclotron
2020: Stage II-a – Basic configuration of the NICA complex
2023: Stage II-b: The full configuration of the NICA complex

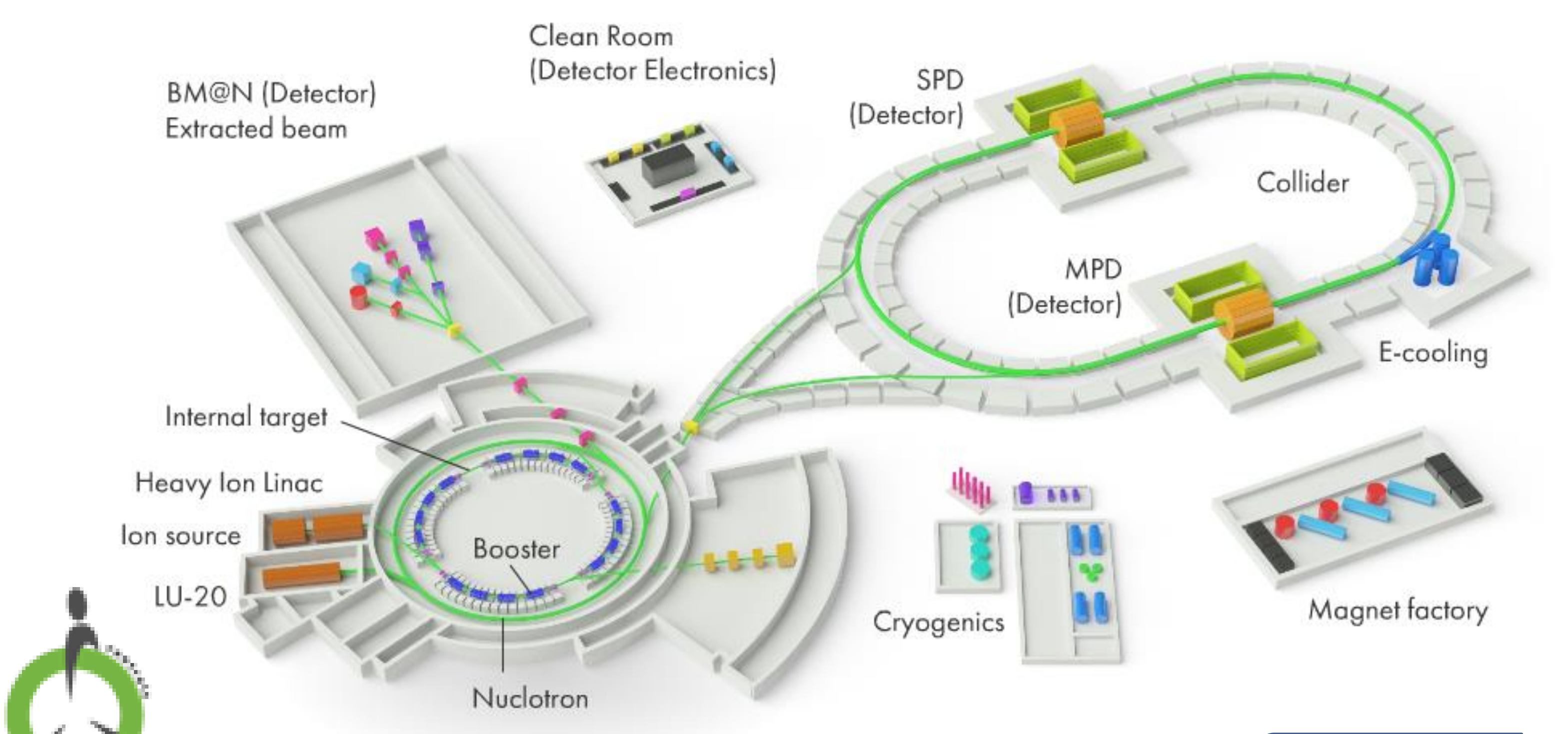


Fig.1 NICA accelerating complex layout

TANGO based control system is under development. Key points:

- **Centralized** administration and monitoring.
- **Reliable** operation, quick recovery after failures.
- **Safe** operation, access restrictions.
- **Ease** of support, modification and scaling.
- **Rapid** development and easy deployment.

TANGO

Control system access control requirements:

- Complement and improve native TANGO client side access control by **additional** server side security checks.
- Centralized management of users and their permissions.
- Flexible access rights.
- Allow TANGO devices to log important information into the central database.
- No complications to both Tango device server and client development.
- No modifications to Tango library.
- Additional protection of TANGO database to track its modifications.

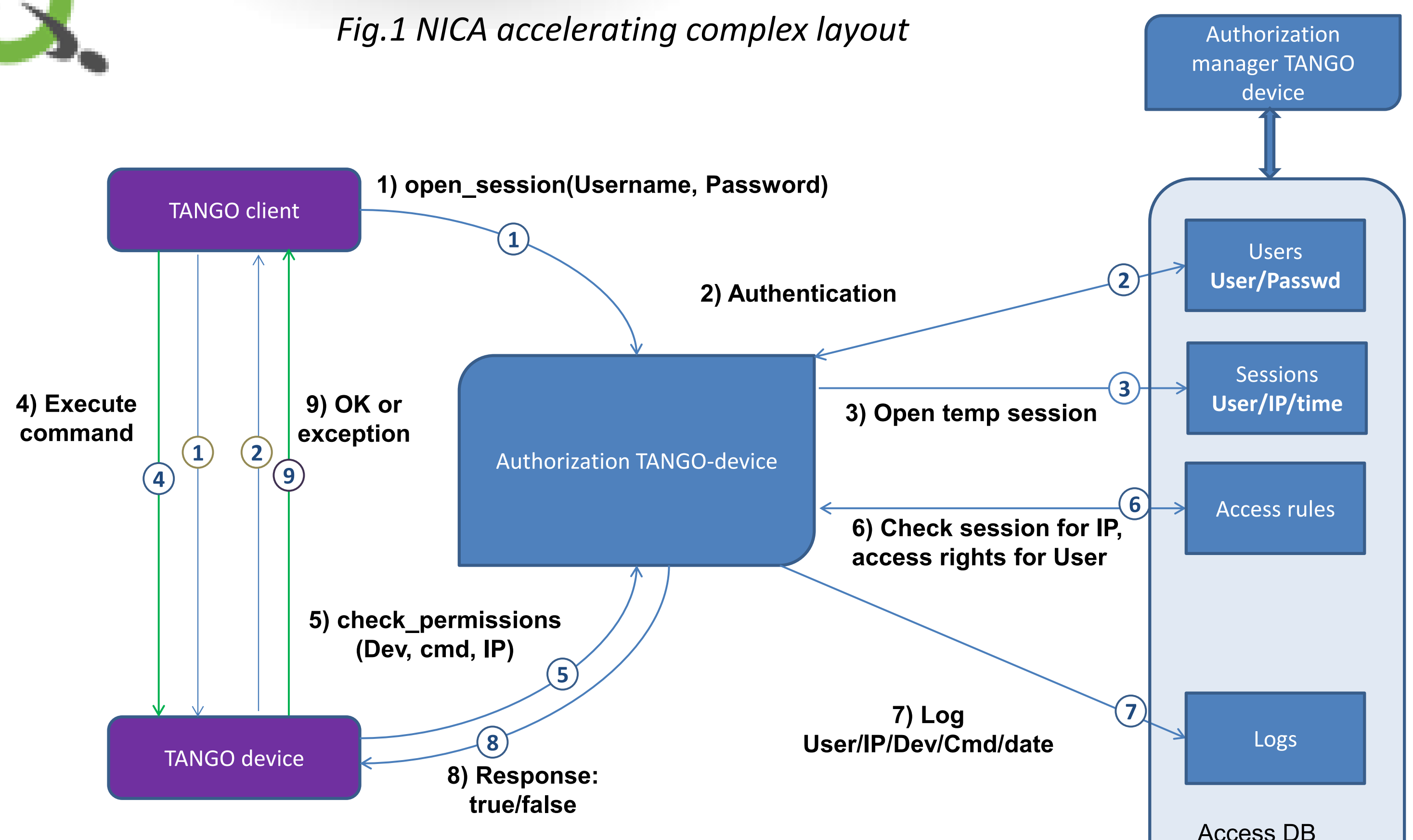
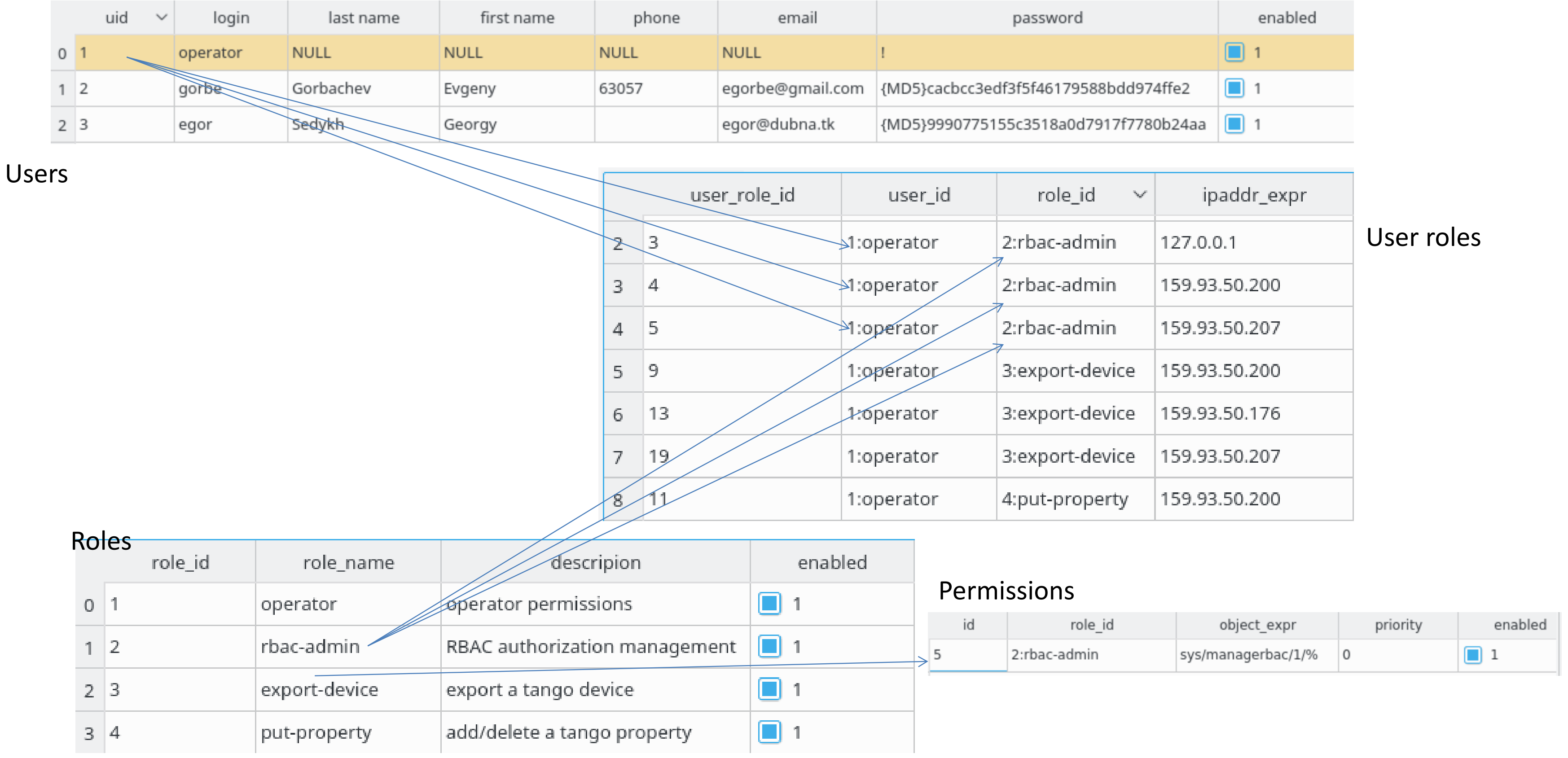


Fig.2 Server side authorization algorithm.

Realization details:

1. Additional TANGO device server to perform authentication, authorization and session management.
2. Role Based Access Control (RBAC):
   - Each role have a group of permissions.
   - Several roles can be assigned to user/IP pair
   - Priorities to separate expert/operator rights.
3. Authentication by location (IP address) and/or username/password.
   - Access from operator's PC and CS core servers without passwords.
4. Support of MySQL regular or wildcard expressions in rules and addresses: can be configured as Tango property.
5. Objects access cache for improving performance.
6. Provide simple interface for TANGO devices to check client's permissions:
   auth=new TangoAuthClientClass(this);
   auth->CheckAccess("cmd_name");
6. Provide authorization for Web clients.
7. Can be easily switched OFF to provide access without access control.
8. Separate TANGO device to manage access control database.



Users

	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 roles

	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

Roles

	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

Permissions

id	role_id	object_expr	priority	enabled
5	2:rbac-admin	sys/managerbac/1/%	0	☑ 1

Fig.3 Role based access control principles.

Tango database protection by using additional TANGO database server with access control and logging:

1. Initialize as TANGO database server
2. Create dynamic commands and attributes copied from original database device.
3. All dynamic commands use the same command class with method execute():

- Check access with command name
- Execute command on original TANGO database device with arguments
- Return result to client or generate exception.

4. The implemented access control allows to restrict modifications of the TANGO database, for example, one can specify computers which can export TANGO devices, add or modify TANGO devices properties and so on.

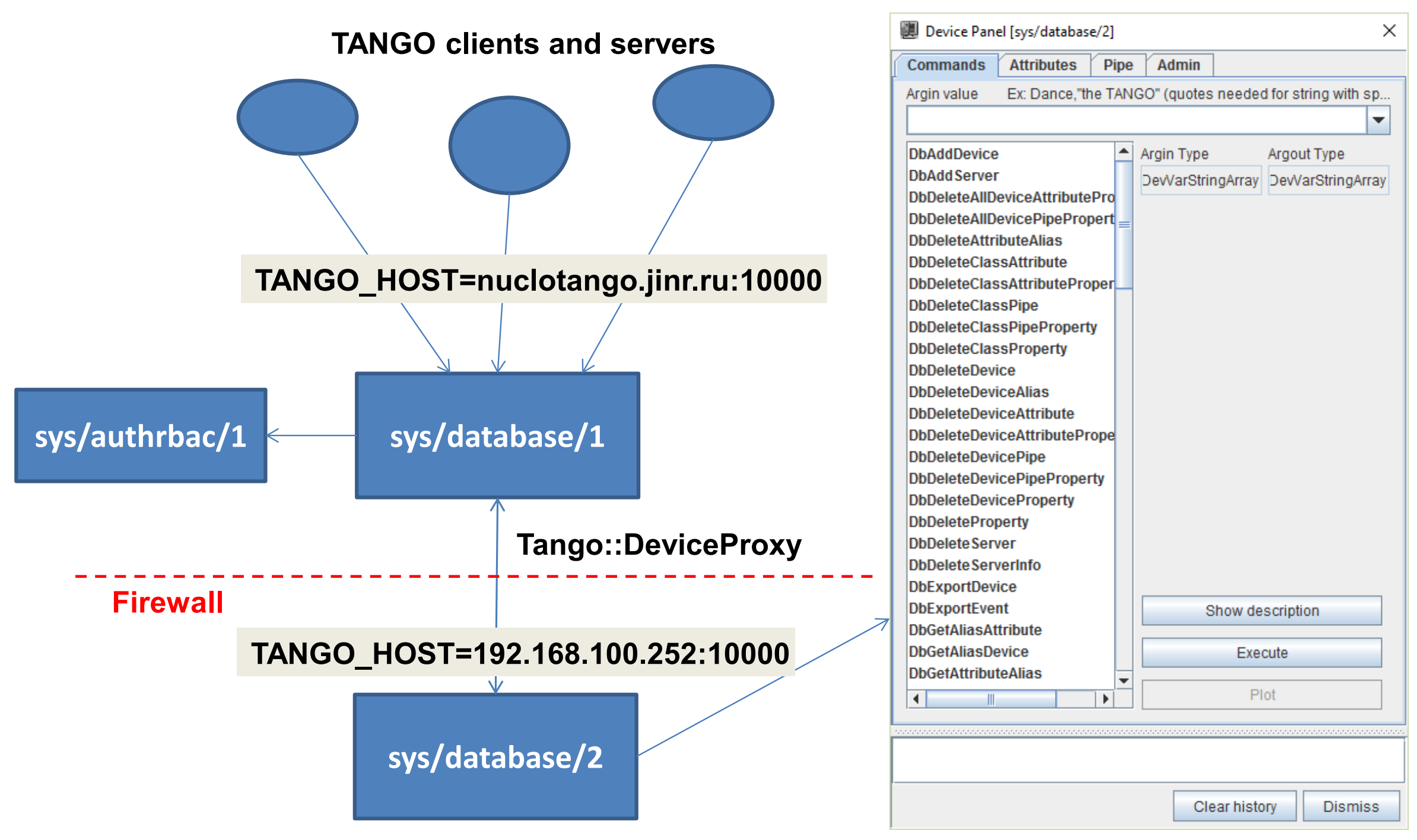


Fig.4 TANGO database server with authorization and logging support

Database server performance tests:

The authorization TANGO device keeps cache of authorization requests allowing to reduce the wildcards and regular expressions evaluation impact on performance. The cache is cleaned automatically by MySQL triggers with the user session expiration. The performance of authorization server and TANGO database server with/without authorization are show in Fig.5 and Fig.6.

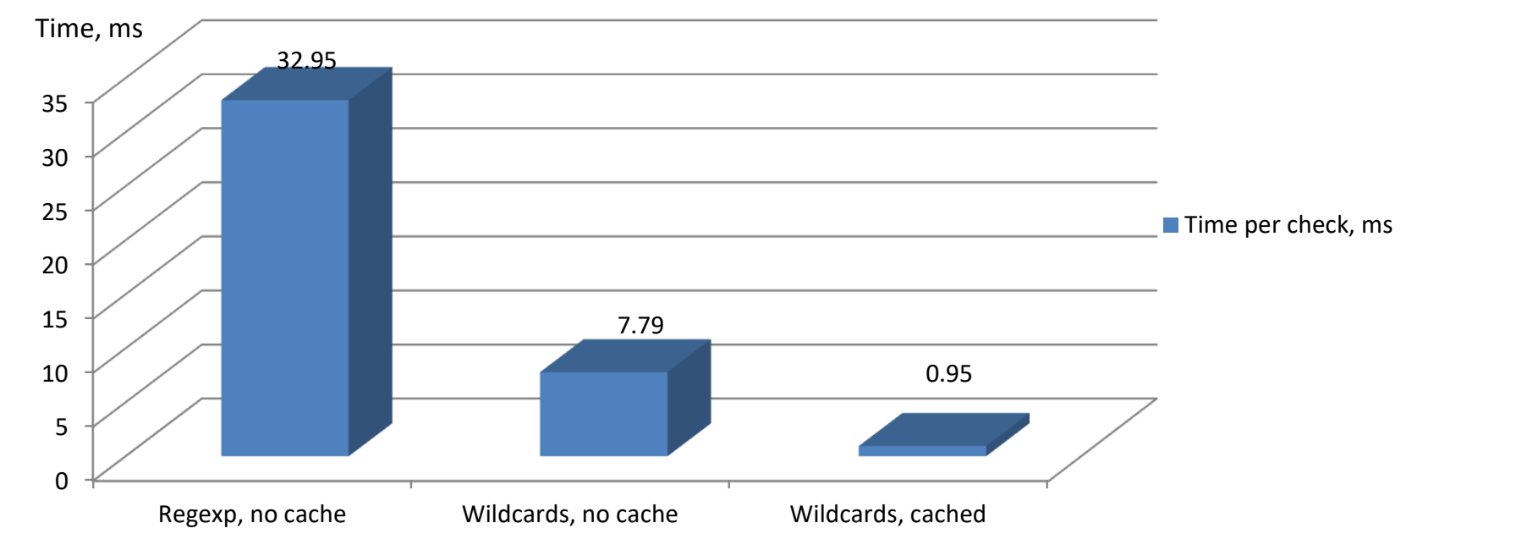


Fig.5 Authorization server performance tests

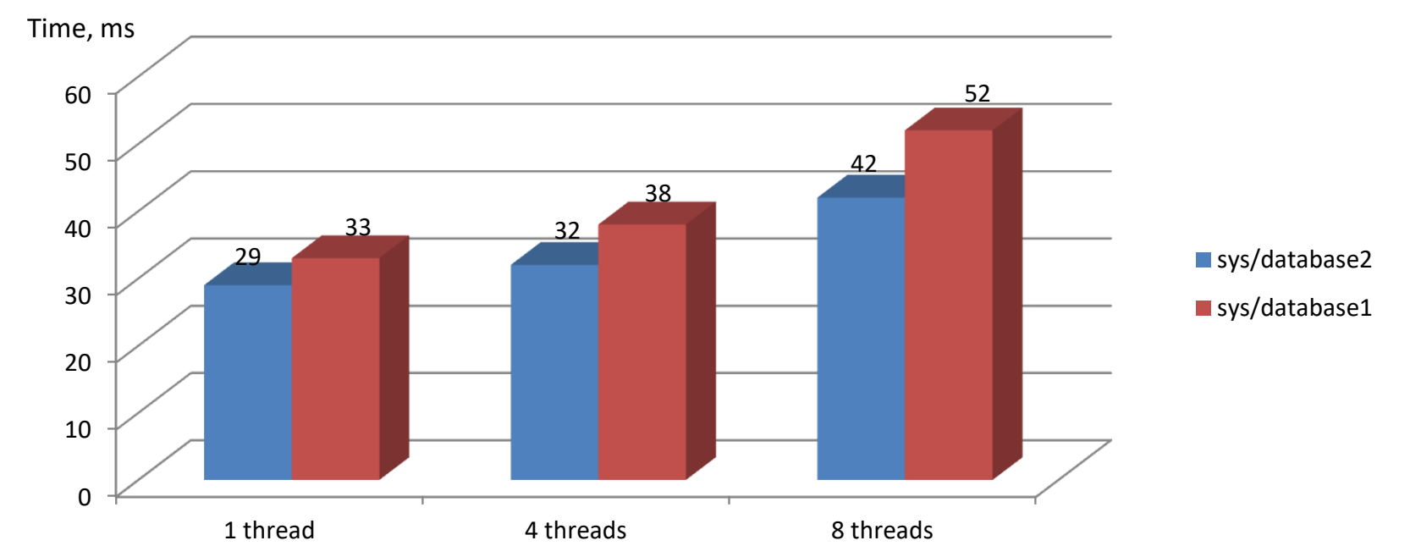


Fig.6 TANGO database server performance tests

Logging:

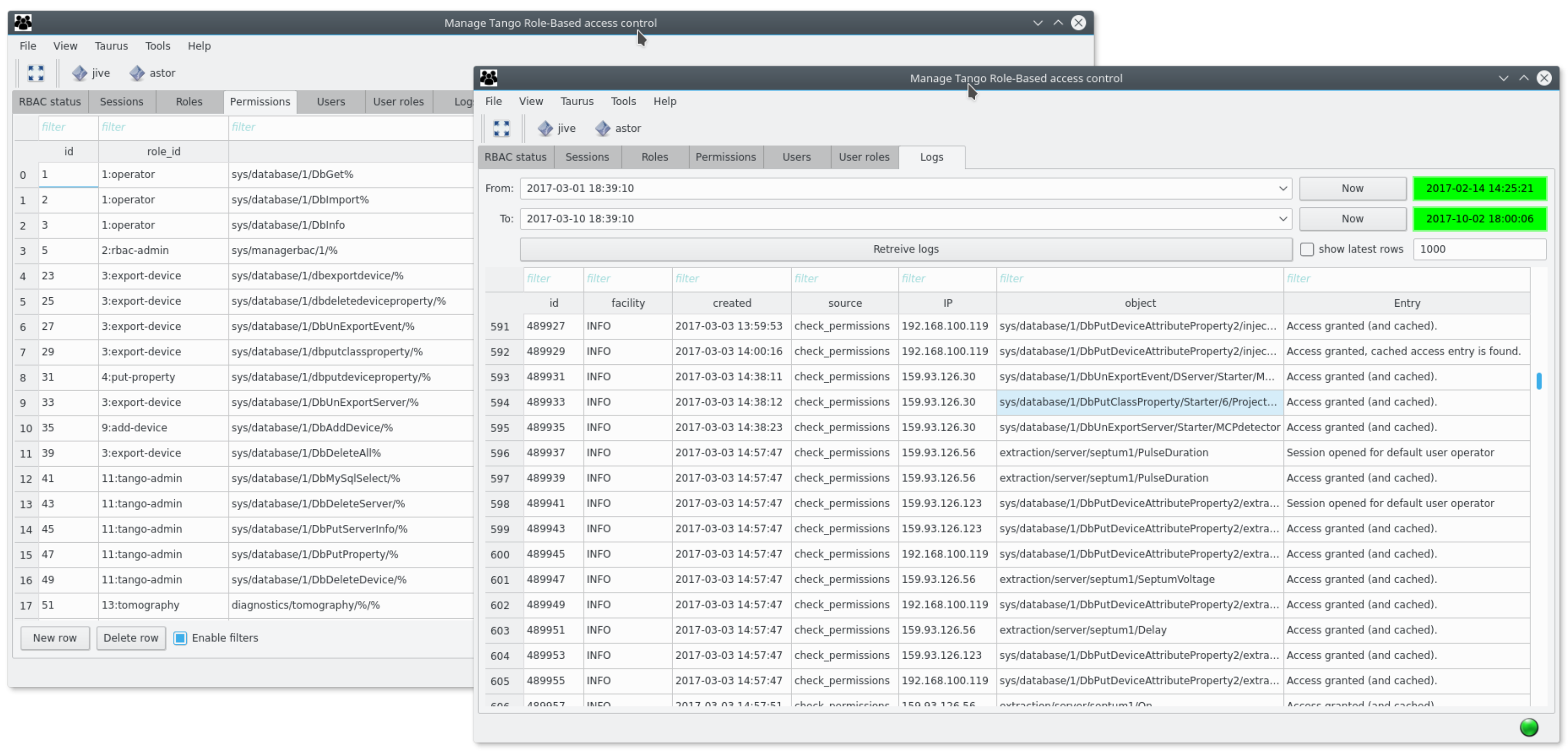
- Full logs of TANGO database changes – exporting devices, changing properties etc.
- Logging can be skipped for certain patterns (via TANGO property) to reduce log data.
- Provide simple interface for TANGO devices to log important information:
  auth->Log("cmd_name", message);
- Flexible interface for administrators to find information in logs (Fig. 7).

Access control system management:

- Special TANGO device to access and edit RBAC database.
- Python Qt client to manage all aspects of the access control database: sessions, users, roles, permissions, state and status of RBAC authorization system, access logs.

Conclusions

The server-based access control system was successfully tested during 54-th Nuclotron run (winter 2017). It provided lots of useful information about control system execution and allowed to find some problems with TANGO devices functionality.



	id	role_id	
0	1	1:operator	sys/database/1/DbGet%
1	2	1:operator	sys/database/1/DbImport%
2	3	1:operator	sys/database/1/DbInfo
3	5	2:rbac-admin	sys/managerbac/1/%
4	23	3:export-device	sys/database/1/dbexportdevice/%
5	25	3:export-device	sys/database/1/dbdeletedeviceproperty/%
6	27	3:export-device	sys/database/1/DbUnExportEvent/%
7	29	3:export-device	sys/database/1/dbputclassproperty/%
8	31	4:put-property	sys/database/1/dbputdeviceproperty/%
9	33	3:export-device	sys/database/1/DbUnExportServer/%
10	35	9:add-device	sys/database/1/DbAddDevice/%
11	39	3:export-device	sys/database/1/DbDeleteAll%
12	41	11:tango-admin	sys/database/1/DbMySqlSelect/%
13	43	11:tango-admin	sys/database/1/DbDeleteServer/%
14	45	11:tango-admin	sys/database/1/DbPutServerInfo/%
15	47	11:tango-admin	sys/database/1/DbPutProperty/%
16	49	11:tango-admin	sys/database/1/DbDeleteDevice/%
17	51	13:tomography	diagnostics/tomography/%/%

From: 2017-03-01 18:39:10 Now 2017-02-14 14:25:21
To: 2017-03-10 18:39:10 Now 2017-10-02 18:00:06
show latest rows 1000

	id	facility	created	source	IP	object	Entry
591	489927	INFO	2017-03-03 13:59:53	check_permissions	192.168.100.119	sys/database/1/DbPutDeviceAttributeProperty2/injec...	Access granted (and cached).
592	489929	INFO	2017-03-03 14:00:16	check_permissions	192.168.100.119	sys/database/1/DbPutDeviceAttributeProperty2/injec...	Access granted, cached access entry is found.
593	489931	INFO	2017-03-03 14:38:11	check_permissions	159.93.126.30	sys/database/1/DbUnExportEvent/DServer/Starter/M...	Access granted (and cached).
594	489933	INFO	2017-03-03 14:38:12	check_permissions	159.93.126.30	sys/database/1/DbPutClassProperty/Starter/6/Project...	Access granted (and cached).
595	489935	INFO	2017-03-03 14:38:23	check_permissions	159.93.126.30	sys/database/1/DbUnExportServer/Starter/MCPdetector	Access granted (and cached).
596	489937	INFO	2017-03-03 14:57:47	check_permissions	159.93.126.56	extraction/server/septum1/PulseDuration	Session opened for default user operator
597	489939	INFO	2017-03-03 14:57:47	check_permissions	159.93.126.56	extraction/server/septum1/PulseDuration	Access granted (and cached).
598	489941	INFO	2017-03-03 14:57:47	check_permissions	159.93.126.123	sys/database/1/DbPutDeviceAttributeProperty2/extra...	Session opened for default user operator
599	489943	INFO	2017-03-03 14:57:47	check_permissions	159.93.126.123	sys/database/1/DbPutDeviceAttributeProperty2/extra...	Access granted (and cached).
600	489945	INFO	2017-03-03 14:57:47	check_permissions	192.168.100.119	sys/database/1/DbPutDeviceAttributeProperty2/extra...	Access granted (and cached).
601	489947	INFO	2017-03-03 14:57:47	check_permissions	159.93.126.56	extraction/server/septum1/SeptumVoltage	Access granted (and cached).
602	489949	INFO	2017-03-03 14:57:47	check_permissions	192.168.100.119	sys/database/1/DbPutDeviceAttributeProperty2/extra...	Access granted (and cached).
603	489951	INFO	2017-03-03 14:57:47	check_permissions	159.93.126.56	extraction/server/septum1/Delay	Access granted (and cached).
604	489953	INFO	2017-03-03 14:57:47	check_permissions	159.93.126.123	sys/database/1/DbPutDeviceAttributeProperty2/extra...	Access granted (and cached).
605	489955	INFO	2017-03-03 14:57:47	check_permissions	192.168.100.119	sys/database/1/DbPutDeviceAttributeProperty2/extra...	Access granted (and cached).
606	489957	INFO	2017-03-03 14:57:51	check_permissions	159.93.126.56	extraction/server/septum1/On	Access granted (and cached).

Fig.7 GUI to manage authorization details and logs

ICALEPCS2017
Barcelona · Spain, October 8-13 · Palau de Congressos de Catalunya
16th International Conference on Accelerator and Large Experimental Physics Control Systems

16th International Conference on Accelerator & Large Experimental Physics Control Systems, October 8-13, 2017, Barcelona , Spain
TUPHA171