WEMMU009

ICALEPCS'11

13th International Conference on Accelerator and Large Experimental Physics Control Systems
October 10-14, 2011, WTC Grenoble, France

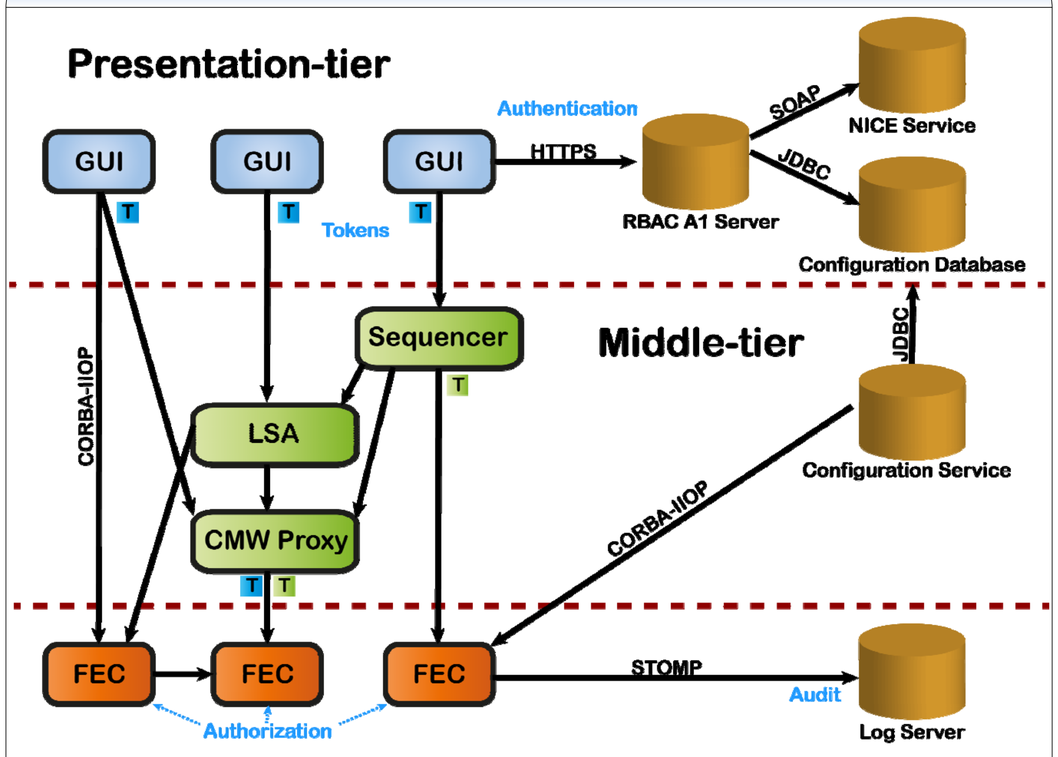
Status of the RBAC Infrastructure and Lessons Learnt from its Deployment in LHC

I. Yastrebov, W. Sliwinski, P. Charrue, CERN, Geneva, Switzerland

Abstract

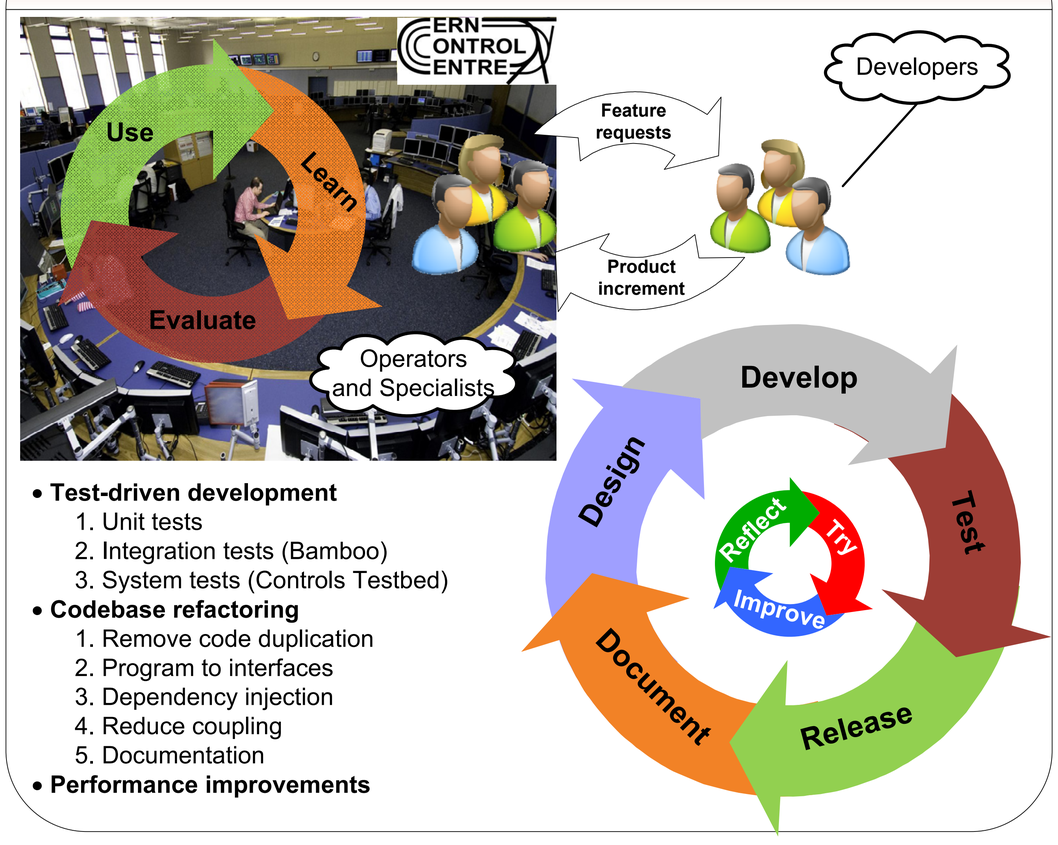
The distributed control system for the LHC accelerator poses many challenges due to its inherent heterogeneity and highly dynamic nature. One of the important aspects is to protect the machine against unauthorised access and unsafe operation of the control system, from the low-level front-end machines up to the high-level control applications running in the control room. In order to prevent an unauthorized access to the control system and accelerator equipment and to address the possible security issues, the Role Based Access Control (RBAC) project was designed and developed at CERN, with a major contribution from Fermilab laboratory. Furthermore, RBAC became an integral part of the CERN Controls Middleware (CMW) infrastructure and it was deployed and commissioned in the LHC operation in the summer 2008, well before the first beam in LHC. This paper presents the current status of the RBAC infrastructure, together with an outcome and gathered experience after a massive deployment in the LHC operation. Moreover, we outline how the project evolved over the last three years and give an overview of the major extensions introduced to improve integration, stability and its functionality. The paper also describes the plans of future project evolution and possible extensions, based on gathered users requirements and operational experience.

Architecture



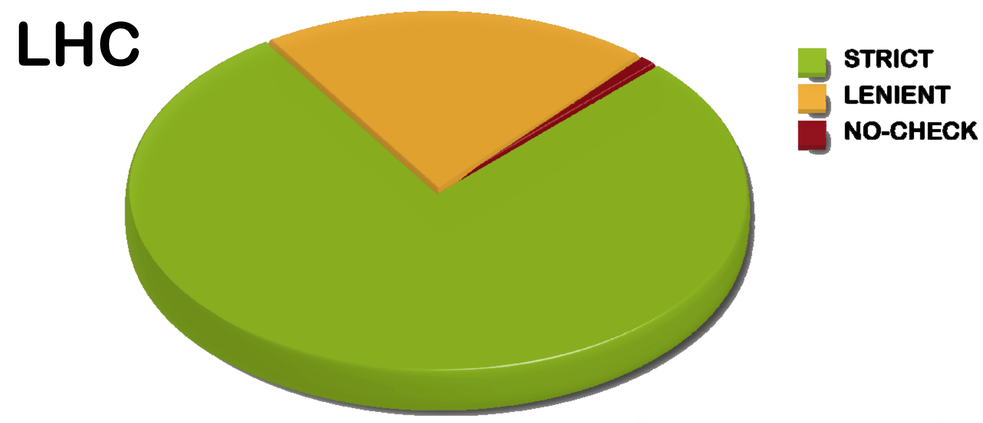
In the *Presentation-tier*, RBAC authentication library was introduced for client applications running in the CERN Control Centre. In the *Middle-tier*, security components provided by RBAC were integrated in the high-level control subsystems and CMW Proxies.
In the *Front-end-tier*, RBAC authorization library integrates with CMW, FESA, FGC & PVSS.

Quality Assurance



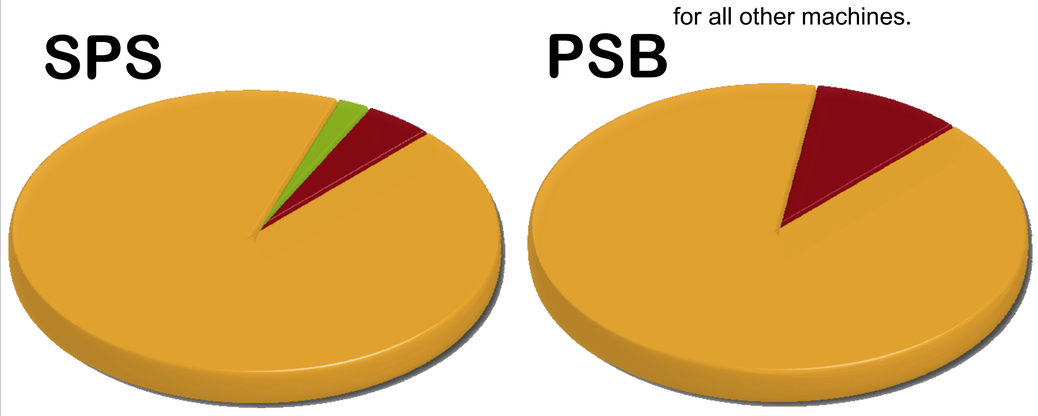
- **Test-driven development**
  1. Unit tests
  2. Integration tests (Bamboo)
  3. System tests (Controls Testbed)
- **Codebase refactoring**
  1. Remove code duplication
  2. Program to interfaces
  3. Dependency injection
  4. Reduce coupling
  5. Documentation
- **Performance improvements**

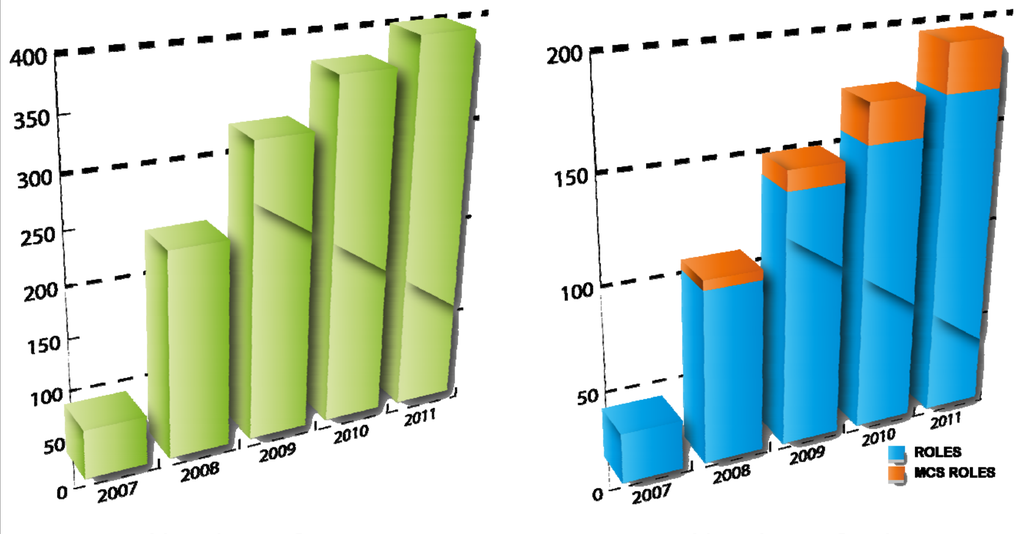
Deployment



Authorization Policies:
- **STRICT** (full protection, authentication is obligatory)
- **LENIENT** (partial protection, authentication is optional)
- **NO-CHECK** (no protection, authentication is optional)

Dynamic authorization allows phased introduction of access control. During deployment campaign STRICT policy was enforced for LHC and LENIENT for all other machines.





Number of users

During deployment campaign in 2008 RBAC was successfully integrated in all layers of the LHC Control System. Since that time the number of RBAC users is constantly growing up because of new client applications and extension of the project applicability.

Number of roles

This diagram demonstrates growing number of user roles over the last years. In 2008 RBAC was extended to provide management of the public/private key pairs (MCS). For MCS roles several additional restrictions were implemented: lifetime constraints and limit of active critical roles.

Conclusions

The RBAC infrastructure was successfully deployed and commissioned in LHC operations in 2008. The feasibility, performance and overhead of RBAC were experimentally evaluated. The results show that the overhead is acceptable and the chosen approach can be effectively used to enforce access control in the CERN Control System. Currently RBAC is used to protect all LHC equipment and selected equipment of other machines. Nevertheless, there are still few areas where current implementation can be extended in order to expand its applicability.

Selected references

[1] S.R. Gysin et al., "Role-Based Access Control for the Accelerator Control System at CERN", ICALEPCS'07, Knoxville, Tennessee, USA.
[2] K. Kostro, W. Gajewski, S. Gysin, "Role-Based Authorization in Equipment Access at CERN", ICALEPCS'07, Knoxville, Tennessee, USA.
[3] Z. Zaharieva et al., "Database Foundation for the Configuration Management of the CERN Accelerator Controls System", ICALEPCS'11, Grenoble, France.
[4] M. Arruat et al., "Front-End Software Architecture", ICALEPCS'07, Knoxville, Tennessee, USA.
[5] W. Sliwinski et al., "Management of Critical Machine Settings for Accelerators at CERN", ICALEPCS'09, Kobe, Japan.
[6] J. Nguyen Xuan, V. Baggiolini, "Testbed for Validating the LHC Controls System Core Before Deployment", ICALEPCS'11, Grenoble, France.