INTEGRATION OF HETEROGENEOUS ACCESS CONTROL FUNCTIONALITIES USING THE NEW GENERATION OF NI cRIO 903X CONTROLLERS

F. Valentini, T. Hakulinen, L. Hammouti, P. Ninin
CERN, Geneva, Switzerland

Abstract

Engineering of Personnel Protection Systems (PPS) in large research facilities, such CERN, represents nowadays a major challenge in terms of requirements for safety and access control functionalities. PPS are usually conceived as two separate independent entities: a Safety System dealing with machine interlocks and subject to rigid safety standards (e.g. IEC-61508); and a conventional Access Control System made by integration of different COTS technologies. The latter provides a large palette of functionalities and tools intended either to assist users accessing the controlled areas, either to automate a certain number of control room operator's tasks. In this paper we analyse the benefits in terms of performance, cost and system maintainability of adopting the new generation of NI multipurpose cRIO 903x controllers. These new devices allows an optimal integration of a large set of access control functionalities, namely: automatic control of motorized devices, identification/count of users in zone, implementation of dedicated anti-intrusion algorithms, graphical display of relevant information for local users, and remote control/monitoring for control room operators.

INTRODUCTION

The GS/ASE group is responsible for the realization and the maintenance of Personnel Protection Systems ensuring the safety of personnel accessing to the various accelerator complexes of CERN. The group was responsible for the conception of a new generation of *access points* [3] to gradually replace the traditional rotating gates, some of them aged of few decades.

Even though the different system functionalities were clearly identified and specified since the beginning of the project, the realization strategy favored a construction by the integration of off-the-shelf (COTS) products rather than to privilege any form of custom development. This choice was mainly motivated by the limited internal resources, making it necessary to externalize the activity to a system integrator, and by the fact that the various functionalities to be provided were already present on the market with well-known and robust commercial solutions. Another motivation was the conviction that constructing a new system out of modular simple blocks would be more easy and rapid than to start a development from scratch. However, in our experience, it turned out that dealing with COTS can be quite a risky activity for a wide variety of reasons.

In [1], presented in the *International Conference on Software Engineering* of 1995, Garlan, et al., introduces the term of *architectural mismatch* to explain the different problems inherent in integration of COTS software components. Typically, many problems are caused by incompatibilities between the programming languages, the operating platforms or the database schemas of the products being integrated. The authors argue that at the origin of any architectural mismatch problem there is the fact that COTS components make several assumptions about the system architecture and its operational environment; consequently, when these assumptions conflict or do not match with each other, the simplicity of assembling complex systems from integration of COTS immediately disappears.

The biggest challenge for designing an access point turned out to be the integration of numerous heterogeneous components such as PLCs to command the movements of the motorized doors, *front-end* to deal with the real-time authorization management, *biometry* for authenticating users, *video system* for remote surveillance of the areas, *public address* system for broadcasting of audio messages, and many other devices. In this context our team is constantly seeking new solutions and technologies allowing to minimize the number of CPUs and information that need to be handled and exchanged between the different subsystems.

This paper will especially focus on the impact analysis that a completely COTS oriented realization strategy had on the architecture of the first series of our access points and it highlights the actual interest in the National Instruments technology [5] as a possible solution for the implementation of more rational system architectures.

THE ACCESS POINT CONCEPT

This section describes the ideas and the concepts behind any access point at CERN. Many would claim that an access point is simply made of "*one door, equipped with expensive position sensors, a video camera and a microphone allowing remote connections with guardians or operators*". However it is much more than that. An access point in a facility like CERN plays a crucial role in defending the installation against intrusions and accesses of people not holding the security requirements. At the same time, it ensures the safety of personnel every-day working inside the potentially dangerous areas.

ISBN 978-3-95450-148-9

Figure 1: Standard configuration of an Access Point.

In order to accomplish its double mission, an access point (see Fig. 1) has to provide a certain number of important functionalities:

- Personnel Access Supervision: a dedicated device (PAD) is in charge of regulating the entrance of personnel. The device is an air-lock closed by 2 motorized doors and equipped with redundant anti-fraud detection systems dealing with all typical situations of piggybacking and tailgating intrusions.
- Material Access Supervision: an additional specific device (MAD) is in charge of controlling the transfer of bulky material to and from the controlled areas. The device is made of two motorized doors that cannot be opened at the same time; the internal volume is then surveilled by two human detection systems based on motion detection and video image analysis algorithms, in order to reduce the possibility for a person to gain easy access to the zone.
- Dynamic Information Dispatch: personnel accessing the controlled areas needs to be dynamically informed about the safety conditions inside the zone. The information system is made up of two independent components: a group of LEDs for critical safety warning visualization, directly animated by a PLC; and a standard local screen hosting a graphical user interface. This latter shows information about the operational state of the zone and it drives users though the complete access procedure.
- User Identification: in order to access the controlled areas every user must be identified and his access privileges must be checked against the central authorizations database. The identification of users is done via an RFid badge reader and a biometric eyes scanner.
- Personnel Safety Tokens Distribution: as additional protection, every accessing user is provided with a safety token that is automatically released by a distributor. The possession of the token ensures that beam operations cannot be reestablished.
- Interphone System: an audio/video communication system allows local users to contact the CERN control room operators.
- Remote Maintenance: due to the large number of access points installed all over the CERN complex, the maintenance team needs to be able to perform a certain amount of operations remotely. Extra functionalities were added afterwards in order to power off individuals controllers, access to detailed diagnostic and operational data or to send specific commands to the different electronic devices.

The resulting architecture is the outcome of a process of integration of different hardware and software subsystems, each one basically in charge for realizing a specific well determined function. Just to give an idea, the main subsystems controlling an access point (LHC type) are:

A control unit (UTL) for PAD: the controller, based on a proprietary OS, is in charge of acquiring the RFid badge ids, verifying the users' credentials in a central database and, additionally, for commanding the PAD motorized doors movements.

A Siemens PLC S7-200 for PAD motors: this PLC is provided by the PAD supplier and it is used to directly drive the door motors according to UTL commands.

A control unit (UTL) for the MAD: the controller, based on a proprietary OS, is dedicated uniquely to command the MAD motorized doors.

A microcontroller for MAD motors: this dedicated electronics, Microchip based technology, is provided and programmed by the MAD supplier and it is used to physically drive the door motors according to UTL commands.

Two control units for biometric: one Linux based PC is in charge of the processes related to the eye scanned image, while another dedicated unit simply checks the authorization on the biometric database and communicates the user identified to the PAD's UTL. This info is sent then to the main control front-end that send it back down to the information screen controller for displaying, locally, the name of the user.

A microcontroller for the key distributor: the distributor is an industrial product coming with its own electronic control system to handle all operations on the keys.

A standard Windows PC: another PC is used to run a specific commercial SCADA software that, communicating with a central front-end, displays all live information for local users. Additionally, this PC runs the detection software that is used to analyze the material passed though the MAD.

A Siemens S7-1200 PLC: this was added during the operational phase to perform simple remote maintenance commands. This was the only practicable solution because of the complexity of modifying any of the other existing controllers at this scope.

An I/O remote Ethernet module: the module was added to allow to the MAD video analysis software to acquire

ISBN 978-3-95450-148-9

the state of the MAD door, since it was not possible to extract this information from the MAD UTL.

MAIN PROBLEMS ENCOUNTERED FOR THE ACCESS POINT DESIGN

What appears the most shocking in this architecture is that basically every functionality of an access point is realized via one or more industrial controllers. Very frequently these controllers are made by powerful electronics units, equipped with sophisticated microprocessors, modern operating systems and provided with data communication protocols (Ethernet, serials RS 485/422, etc.) as with digital or analog input output interfaces. So, in principle, almost any of the controllers could be programmed to execute the whole set of functions instead of being underutilized and, despite all this, the implementation of some basic functions (as displaying on the local screen the name of last identified user) has turned out to be extremely difficult.

Another critical point is represented by the system maintainability due to the large number of access points actually in operation. Considering a total of 56 units between the LHC and PS with an average of 10 critical controller each, estimating a gross MTBF of 3.4 years for every component, an average time to repair of 3 hours at two technicians: this leads to a total time of **987** working hours per year only for dealing with failures. Additionally to that, extra costs for preventive maintenance (e.g. installation of Windows security patches) have to be considered.

From our point of view many difficulties that are found during the integration of commercial COTS are caused by typical architectural mismatch problems. The attention to a certain number of factors and initial assumptions is essential to avoid a large amount of problems:

1. *Assumptions about the nature of components.*
2. *Evaluation of the communication needs between the different components.*
3. *Flexibility and evolution requirements.*
4. *Maintainability requirements.*

After the return of experience obtained by the design, the construction and the maintenance phases over the past 8 years [3], many efforts have been made in order to find new concepts and methodologies allowing to simplify and homogenize our systems. A second more robust generation of access points have been recently put in operation to regulate all accesses of the PS accelerators complex. Despite that the hardware and software architecture has been entirely reviewed and that the final product presents evident improvements [4], a certain complexity is still affecting the system. The heterogeneity of the various functionalities still requires that a large number of controllers and software products operate together.

CURRENT PRESPECTIVES

Currently, a promising compromise solution between integration of existing components and custom development is offered by the *National Instruments* (NI) technology [5]. This especially thanks to the synergy offered by two NI products: the new generation of Compact RIO 903x controllers and LABVIEW as software development environment.

The typical CompactRIO system is a combination of a real-time controller, reconfigurable I/O Modules and an FPGA chip (see Fig. 2). The real-time target includes an Intel microprocessor for implementing network communication, data logging, control algorithms, and it provides support for deterministic execution thanks to the presence of a real-Time OS. The FPGA module, from Xilinx, is integrated in the same chassis of the microprocessor but it is completely independent; it is commonly used to implement high-speed controls, inline data processing, or complex timing and triggering operations, but also to realize interlocks and digital signals logics [2].

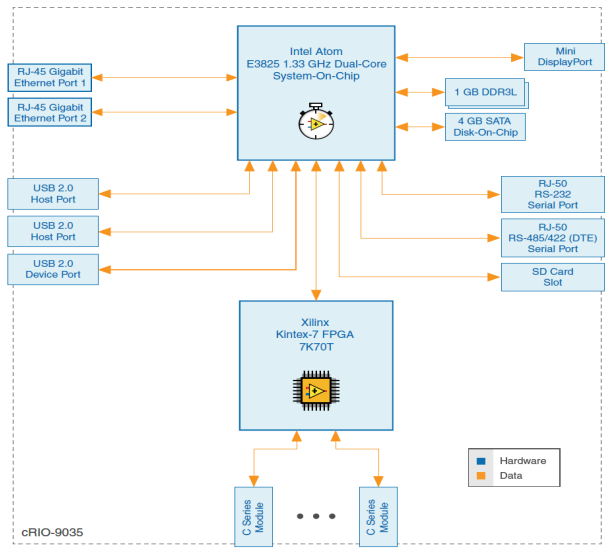

Figure 2: NI cRIO RT & FPGA internal schematics.

The new generation of Compact-Rio controllers (903x family) are particularly interesting due to the fact that NI replaced their proprietary OS with a new version based on Linux Real-Time. This adds much more flexibility to the controller; on one side allowing users to run their own software in parallel with the LABVIEW applications; on the other side it offers the possibility to interface the C-Rio with a wide palette of devices such as: USB keyboard, USB mouse, video monitors, smart cameras, etc. as is usually done in any standard Linux machine.

The second element that makes it possible to employ the cRIO controller to a wide palette of application is offered by LABVIEW. It consists of a graphical software development environment allowing one to construct complex software applications by simply composing and connecting together "*ready-to-use*" blocks. The predefined palette of connectable blocks is very wide and it contains solutions for the most common exigencies of software developers, as: file management, database connections, OPC communications, physical I/O controls, image pro-

ISBN 978-3-95450-148-9

cessing, complex vector/matrix manipulation, mathematical analysis, etc.

SOME INITIAL FEEDBACKS

At the present time our team is studying the possibility to drastically reduce the complexity and the amount of electronics required for access point control by adopting the NI cRIO 903x as unique controller. A real scale prototype is under construction, but we have already some feedback on a certain number of core functionalities that were developed in LABVIEW and tested on a cRIO 9030.

Displaying of local information HMI: the new cRIO 903x series is equipped with a HDMI video output port that is perfectly suitable to drive a local screen. Some test GUI applications have been easily realized via LABVIEW in order to test the large palette of graphical components available.

OPC UA data server / remote supervision: the OPC UA server is the solution adopted to make the cRIO communicate with the external world. LABVIEW allowed us to realize a first test application by just connecting a total of 11 predefined blocks to implement an OPC UA server. This sends periodically monitoring data, computed or acquired by the controller, to Technical Infrastructure Monitoring system, that is one of the main SCADA supervision tools for the operators of CERN control room.

Connection to Oracle databases: connections to the authorizations database are performed in order to verify the users' access privileges and to verify a certain number of conditions (e.g. valid activity permit). These functionalities, currently realized by a dedicated electronics (UTL), can be easily programmed in LABVIEW in order to be executed in the cRIO. This is realized thanks to the database toolbox inside the LV *connectivity* package. An interesting possibility to be investigated is the installation, directly on the cRIO Linux real-time target, of a local database instance, anyone suitable for Linux environment (e.g. MySQL). This would allow to store locally a copy of the relevant central database tables so as not to be affected by network cuts or other problems.

Image processing & intrusion detection: the software for video analysis in charge of detecting unauthorized presence of personnel inside the Material Access Device (MAD) has been rewritten in LABVIEW in order to be executed directly on the cRIO real-time target. The exercise was particularly interesting because, thanks to the richness of functionalities offered by the image processing toolboxes, we obtained a very simplified implementation of the software. Contrary to the actual C++ implementation, the LABVIEW version of the software meets much more closely maintenance and evolutionary requirements.

Badge RFid acquisition: Tests to control a STid RF badge reader have been successfully performed using the VISA objects inside the *Data Communication* tool box. The model of RFid reader in use at CERN is of type ISO 15693 (13.56 MHz) and connected via a serial RS485 link. The simple application developed in LABVIEW showed that the control of a standard CERN badge reader was possible and very easy to realize, simply via the connections of a few blocks.

Additional functionalities providing the physical control of PAD and MAD motorized doors, of key distributors and various other devices have to be still implemented, furthermore, performance and robustness tests have to be conducted during several mounts.

CONCLUSIONS

The choice between a fully COTS assembly activity against a more optimized integration, including *in-house* developments, is driven by several evaluation criteria, of which the principals are in relation with:

- Evaluation of available internal resources;
- Time to develop, document and fully qualify certain functionalities;
- Level of complexity of the system in terms of HW/SW components and their interconnections.
- Sustainability of annual maintenance costs.

The REX, gained after several years of system integration, has however highlighted that to gain in maintainability and evolutivity a simple COTS integration may be not sufficient and new concepts or more advanced integration tools needs to be considered. The exigencies for obtaining a system capable of performing heterogeneous functionalities being, at the same time, flexible, capable to host new functional requirements, easy to maintain and to develop prompted us to consider another integration principle, based on National Instruments solutions, for the next generation of access points.

The present prototyping activity showed that the utilization of the CRIO 903x controllers, in combination with LABVIEW development environment, could be suitable for our needs. Although more data is essential to better evaluate performances and robustness of this technology, the first results obtained with NI are encouraging to pursue this investigation.

REFERENCES

[1] D. Garlan et al., "*Architectural Mismatch or Why it's Hard to Build Systems out of Existing Parts,*" Proc. 17th IEEE/ACM, Seattle (USA) 1995.

[2] T. Hakulinen et al., "*Building an Interlock: Comparing Technologies for constructing Safety Interlocks*," MOPGF143, Melbourne (AU), these proceedings.

[3] T. Ladzinski et al., "*Access Safety Systems - New Concepts from the LHC Experience*," ICALEPCS11, Grenoble (FRANCE), WEPMU008, 2011.

[4] P. Ninin et al., "*Refurbishing of the CERN PS Complex Personnel Protection System*," ICALEPCS13, San Francisco (USA) 2013.

[5] http://www.ni.com

ISBN 978-3-95450-148-9