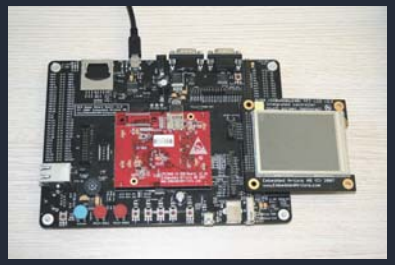
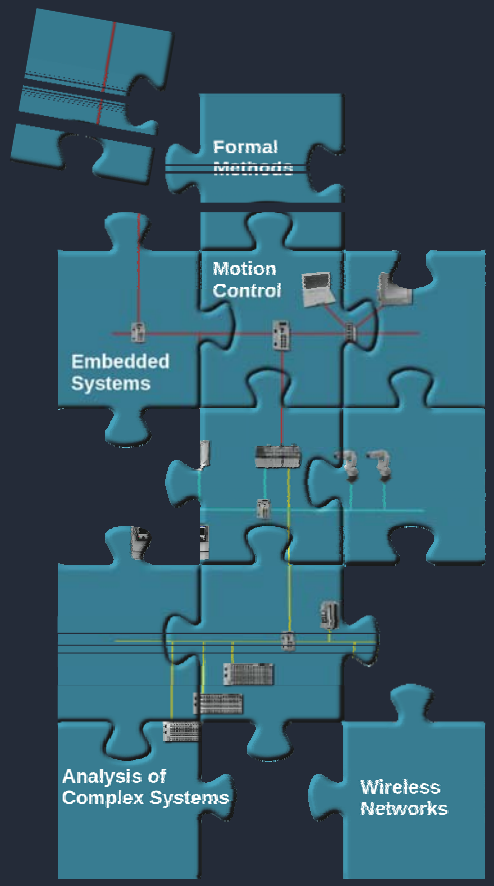
Real-Time and Embedded Systems

Adopting a real-time operating system (RTOS) for embedded applications development is becoming increasingly important, because it is nowadays essential to integrate a large set of heterogeneous, reusable software modules into a single computing system, with as little effort as possible. This certainly occurs in most mobile communication devices, which must execute tasks with tight real-time constraints, like those managing the interaction with the communication network, along with sophisticated general-purpose applets, such as web-browsers and e-mail clients. However, the same is also true for many embedded controllers that must now offer, for instance, very complex graphics user interfaces and Internet connectivity for remote management and diagnostics.



The advantages of this trend in terms of software flexibility, reliability and reusability are clear but, until recent times, it was hindered by the high cost and hardware requirements of RTOSs. With the advent of open-source software and the improvement of microcontrollers this is no longer an issue, but a considerable amount of expertise is still needed to deliver a sound design. Most research activities performed by CE&NG in this field, dating back to about 1985, are made at the request of private companies looking to improve their product line. The application domains considered so far include digital satellite/cable TV set-top boxes, smartphones, and distributed industrial controls.



COMPUTER ENGINEERING AND NETWORKS GROUP

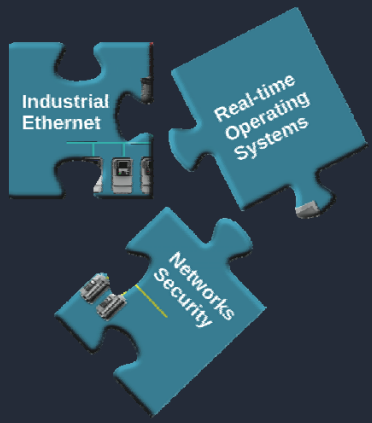
C.so Duca degli Abruzzi 24
10129 Torino, Italy

Phone (+39) 011 090 5410
Fax (+39) 011 090 5429

Info: ceng@ieiit.cnr.it
Web: http://ceng.ieiit.cnr.it

Consiglio Nazionale delle Ricerche
Istituto di Elettronica e di Ingegneria dell'Informazione e delle Telecomunicazioni

COMPUTER ENGINEERING AND NETWORKS GROUP



CE&N group

The Research Group

The Computer Engineering and Networks Group (CE&NG) has acquired considerable experience and know-how in more than three decades devoted to scientific research in the ICT domain.

In the 80s, at the beginning of its activity, the Group mainly focused on local area networks and communication protocols.
The evolution of computers and networks, however, led the CE&NG researchers to extend and refine their scientific interests to other rapidly emerging research areas, including Industrial Communication Systems, Network Security and Real-time and Embedded Operating Systems.

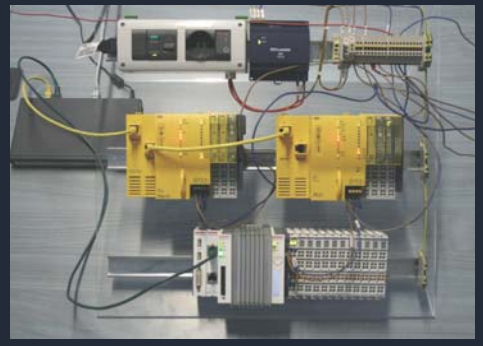
Nowadays, most of the Group scientific activities are located in the computer and communications domains. For instance, CE&NG is deeply involved in the study, development and experimentation of real-time communication technologies, wired and wireless industrial communication networks, small open-source real-time systems, virtualization techniques, formal methods and automated techniques for the analysis of complex systems, s/w tools for the verification of security properties of cryptographic protocols and networks.

CE&NG research activities are mainly oriented to cutting-edge applications in many areas of engineering, and are often carried out in strict cooperation with other authoritative academic organizations, large companies and SMEs, in the framework of Italian and international research projects.

CE&N group

Industrial Communication Systems

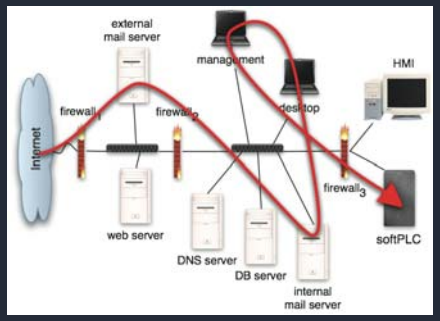
One of the keys to success in modern enterprises is the ability to integrate effectively and inexpensively all activities in production plants. The trend to the widespread adoption of digital communication technologies in factory automation environments dates back to the 80s, with the introduction of fieldbuses. However, convergence towards fully integrated systems, with pervasive adoption of ICT solutions, has just started. Technologies such as industrial Ethernet and wireless networks, just to mention two of them, are going to change deeply the way production is conceived and carried out, with an unprecedented degree of flexibility, scalability and availability.
Despite a number of solutions are already available off-the-shelf, that can be included in both existing and new plants, the situation is far from reaching a steady-state condition. The chance of having a number of functions, originally implemented by different subsystems (e.g. distributed I/O, motion control, supervisory control, diagnostics and safety), which share the very same wire, poses a number of challenges that have to be tackled and solved right in the design phase of production plants, when the most suitable technologies have to be selected.



CE&NG researches focus on these advanced topics and also pay particular attention to national and international standardization activities.

Techniques and Tools for Network Security

Nowadays, industrial plants and critical infrastructures for the production and delivery of services and goods, such as food, electric power, gas, oil and water, are moving from isolation and closed/proprietary communication solutions, typical of the past, to more open, flexible and cheaper standard communication facilities, such as the Internet and its well known media, protocols and services. This migration, however, also exposes those networks to well-known security threats that have been experienced by traditional computer systems. Unfortunately, on the one hand, industrial networks often lack adequate security policies and mechanisms while, on the other hand, some of the well-assessed security techniques, that are popular in the traditional ICT domain, are frequently in contrast with basic requirements of industrial processes and/or incompatible with the low computational power of many industrial devices.



The design and management of security solutions for this kind of networks can profitably take advantage of CE&NG analysis techniques and automated s/w tools. Our solutions can be of significant help in modelling the system, which can even consist of thousands nodes, evaluating the effectiveness of the approach with respect to the functional requirements and security goals, and, consequently, highlighting security weaknesses.