Barilla chooses Siemens to implement Digital Connectivity at its sauce plant in Rubbiano

Barilla, an Italian company founded in 1877 and based in Parma, is the world leader in the food and pasta goods sector and produces pasta, sauces, and baked products at various production sites both in Italy and abroad. Its newest plant is in Rubbiano (PR) and is the only one used to produce sauces, dressings, and pestos, which includes its flagship product: Pesto alla Genovese with fresh basil and Parmigiano Reggiano cheese. The ingredients, recipes, technology, and "know-how" are 100% Italian, as well as the meat, which is sourced entirely from animals reared in Italy, with full traceability.

Highlights of the solution

- Elimination of times of inactivity
- Real-time analyses of huge amounts of data
- More effective way of working thanks to remote control and teleservice
- Repaid investment
- Maximum cybersecurity and data protection standards

SIEMENS

siemens.com/industrial-communication

Built in 2012, the plant was subject to expansion in 2018, which saw the introduction of an additional two lines, doubling production capacity to 120,000 tons of sauce per year.

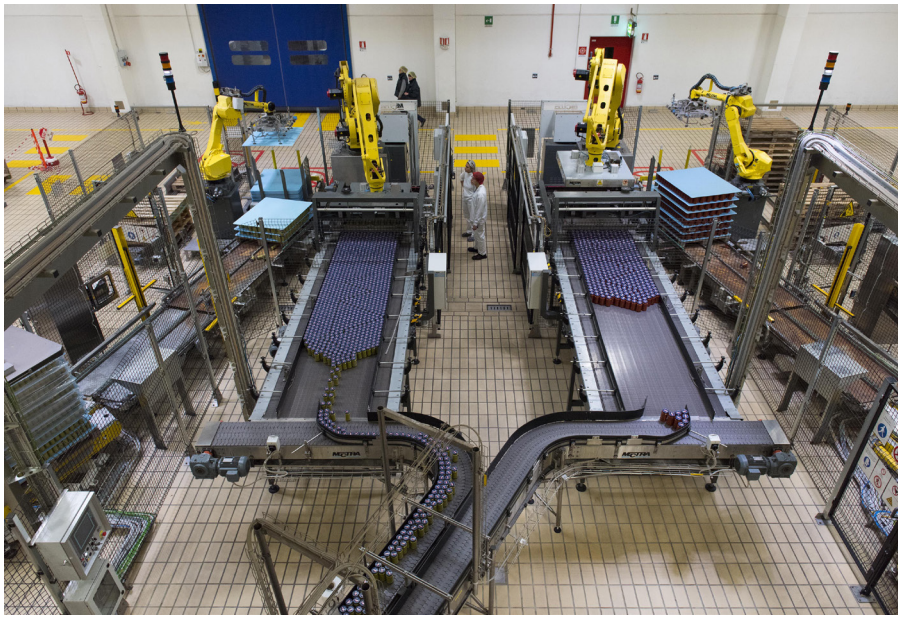
The plant comprises three macro departments, one for cooking, one for production, and one for packaging. In cooking, the different ingredients that go into the sauces are blended together and then cooked inside cookers. The prepared sauces are then sent to the packaging department.

The challenge: automation and state-of-the-art remote control without any downtime

The expansion of the plant goes along with an ever greater proliferation of networked field devices whose task it is to exchange data with SCADA systems and plant management software. It was therefore necessary to develop a robust and organized industrial communication network to ensure the necessary scalability and flexibility to manage the new technology currently on the market in order to be able to archive, process, and analyze the huge amounts of field data (Big Data) in real time and thus allow companies to generate values using this data. The introduction of new cybersecurity standards in an industrial setting, such as the IEC 62443 standard, also prompted the client to revise its industrial network standards.

The plant also required a remote control and teleservice system for the devices that can guarantee both simultaneous technical interventions by suppliers and security, in terms of access control and monitoring. The aim was to transform an uncontrolled access system consisting of a flat network of communication into a network that, by the end of the project, is segmented and structured using a state-of-the-art access method.

Another challenge was to avoid downtime situations and hence prevent disruption of production, as Andrea Di Nicola, Automation Manager at the Barilla plant in Rubbiano, explains: “A key issue for this project has been the implementation of Siemens’ teleservice infrastructure, based on the SINEMA Remote Connect solution combined with the SCALANCE S firewall. The most difficult part was converting the network architecture while the systems were in operation or in the few times production could be shut down. Thanks to the expertise of Siemens and their competent partner ITCore, we managed to achieve this with zero downtime, thanks to the careful management of the operations and network configurations, which made the transparent and optimally controlled transition phase possible. Both companies helped us throughout all the phases of the project, from the start right up to the final training part, the plant’s technical area and maintenance, thus creating a harmonious infrastructure.”



Barilla’s production gains advantages from a new OT network.

Innovative OT network meets high cybersecurity standards

The partnership with Siemens comes along in a natural way: the collaboration between Barilla and Siemens has been producing winning results for years. This is where the strong motivation was born to continue in this way and prefer Siemens over other automation companies. "Our trump card has been the full participation and collaboration in the pre-analysis phase and technical and economic assessment of the investment with Siemens, right from the start," continued Di Nicola. "We tackled this project together. The main idea was to get the worlds of IT (information technology) and OT (operational technology) talking, as before this project the whole automation network in the factory was almost entirely the domain of IT Barilla. The aim of this project was to separate the IT world from the automation world whilst at the same time making them interface in a functional way."

In fact, Siemens recommended to Barilla the most innovative OT networking and cybersecurity technologies currently on the market, ensuring complete compatibility of Siemens' devices with regard to systems and components from other automation suppliers.

The strength has been the components and competence offered by Siemens and the possibility to easily manage communications from other vendors, guaranteeing adequate continuity of production.

Marcello Scalfi, Sales Specialist Team Leader Digital Connectivity and Power at Siemens Italia, notes: "Integration work between the information technology and operation technology teams, carried out by Siemens, required a long internal evaluation phase together with Barilla, who considered various solutions presented by us via training workshops targeted at Barilla colleagues in the engineering and OT departments for the purpose of increasing their networking and cybersecurity skills. Knowing the technology available has also enabled them to acquire the right skills to be able to assess the best solution to adopt. For Siemens, it was essential to open up the discussion to the possible scenarios so the client could make a conscious choice. It has been an important transition, a training ground for everyone involved."

New network to safeguard production continuity

The whole project was carried out by three parties: Siemens, Barilla, and ITCore.

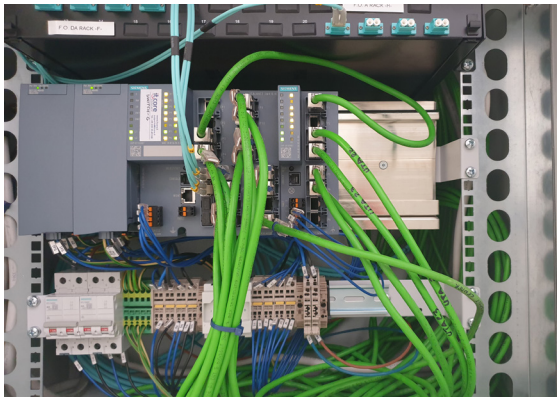
ITCore, as solution partner of Siemens for the strength networks part, has taken a central role in the planning, realization, and maintenance of the whole network infrastructure and the teleservice systems installed at the Rubbiano plant.

The new network, structured with rules and routing plans, now has more than 1,000 interconnected intelligent nodes. The process envisaged the creation of a fiber optic ring backbone network (also called "backbone") managed with MRP (media redundancy protocol) and the segmentation of the automation network in VLAN (Virtual LAN) split into production cells.

Each of these cells is segregated from the others in terms of network and communicates using the following devices from the SCALANCE product family at Siemens:

- Industrial firewalls: a system for network security that allows monitoring of incoming and outgoing traffic using a predefined series of security regulations to allow or block events.
- Industrial switches: network devices responsible for switching at datalink level, which is used to manage the data traffic when there are more connected nodes, separating the so-called collision domains connected to its ports.
- Routers: electronic devices that route data between the networks, distributing the connection between different terminals.

SCALANCE SC632: the array of industrial firewall enables the right communication path from plant network to IT and vice versa.



SCALANCE XM416-4C: the core of the production backbone that provides high availability and redundancy to the plant network.

To complete the solution, a centralized management and control system for remote access to the production network (teleservice) has been integrated according to a defined double jump host model. The implementation of the solution was made possible with the functionality provided by the SCALANCE S equipment from Siemens (industrial firewall) used upstream of the cells and the use of the SINEMA Remote Connect software.

Networking and cybersecurity in the industrial sector are themes that ITCore deals with on a daily basis together with Siemens. “We believe that in the coming years constant monitoring of all devices connected in the network will be essential because, while we cannot think of stopping the digitalization process, we must do everything possible to safeguard production continuity, both in terms of functional operation and protecting the data generated,” states Federico Tarzia, Chief Technical Officer of ITCore.

Results above expectations

The solution put in place by Siemens has made it possible to achieve higher cybersecurity and data protection standards at a factory networking level feasible to date. This makes the Rubbiano plant a real role model for the brand's other plants.

As well as easy maintenance and thus the plug & play replacement of components, and consequently the reduction/elimination of downtime due to malfunctions, another point that has been gaining ever greater value over time and which has made it possible to repay Barilla’s investment in full has been the support. “With the spread, on the one hand, of the pandemic and the necessity to guarantee plant production on the other, investing in a reliable teleservice infrastructure has allowed us to “be in the factory” even if off-site, when smart working,” comments Di Nicola. “At the same time, equipment suppliers, who were not always able to go to the factory to make any changes or interventions due to the pandemic, could use teleservice to be in environments that are segregated from each other, guaranteeing information confidentiality between one supplier and another.” The timely control of this access and the possibility to smoothly control and manage external supplier operations has been another successful aspect of this project.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept. For additional information on industrial security measures that may be implemented, please visit
www.siemens.com/industrialsecurity

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

Reference
PDF 1021 5 En
Produced in Germany

List of Siemens products

- SINEMA Remote Connect
- SCALANCE SC600 router/firewall
- SCALANCE XR500 router/switch
- SCALANCE XM400 switch
- SCALANCE XC200 switch

siemens.com/industrial-communication