Referenz

Barilla beauftragt Siemens mit der Einführung von Digital Connectivity in der Saucen-Fabrik in Rubbiano

Das 1877 gegründete Unternehmen Barilla mit Hauptsitz in Parma ist als weltweiter Marktführer in der Lebensmittel- und Teigwarenindustrie bekannt. An zahlreichen Standorten in und außerhalb Italiens stellt Barilla Nudeln, Saucen und Backwaren her. Das jüngste Werk in Rubbiano ist die einzige Produktionsstätte, in der unter den hergestellten Saucen, Dressings und Pestos regelmäßig auch das Flagschiff des Unternehmens vom Band läuft: Pesto alla Genovese mit frischem Basilikum und Parmigiano Reggiano. Die Inhaltsstoffe, die Rezeptur, die Technologie und das „Know-how" sind zu 100 % italienisch. Ebenso wie das verwendete Fleisch, das ausschließlich von Tieren stammt, die in Italien gezüchtet werden – mit vollständiger Rückverfolgbarkeit.

Highlights dieser Lösung

- Eliminierung von Stillstandszeiten
- Echtzeitanalyse sehr großer Datenmengen
- Effizientere Arbeitsweise dank Fernzugriff und Teleservice
- Investment amortisiert sich
- Höchste Standards an Cybersecurity und Datensicherheit

SIEMENS

siemens.de/industrial-communication

Bereits sechs Jahre nach seiner Eröffnung im Jahr 2012 wurde das Werk in Rubbiano 2018 um zwei zusätzliche Produktionslinien erweitert. Die Produktionskapazität verdoppelte sich in diesem Zuge auf insgesamt 120.000 Tonnen Saucen pro Jahr.

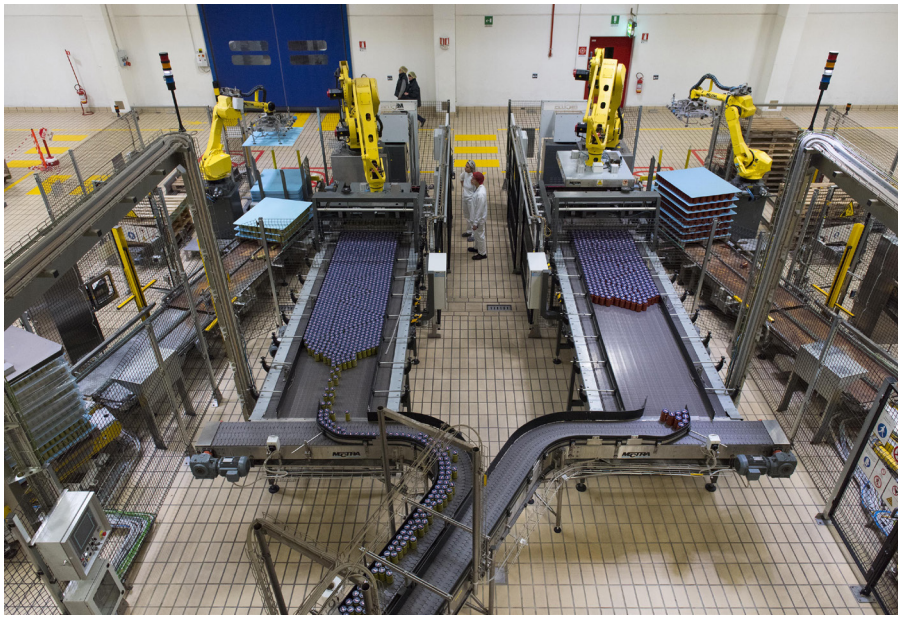
Das Werk ist in drei Großbereiche unterteilt: der Bereich „Kochen", die Produktion und die Verpackung. Im Bereich „Kochen" werden die verschiedenen Inhaltsstoffe der Saucen gemischt und in Kochern gegart. Die fertig vorbereiteten Saucen werden anschließend an die Verpackungsabteilung weitergeleitet.

Die Herausforderung: Automatisierung und moderne Fernsteuerung ohne Standzeiten

Die Erweiterung der Produktionskapazitäten bringt einen stetig wachsenden Anstieg von Feldgeräten mit sich, deren Aufgabe es ist, Daten mit SCADA-Systemen und Betriebsführungssoftware auszutauschen. Es war daher notwendig, ein belastbares und organisiertes industrielles Kommunikationsnetzwerk aufzubauen, welches die notwendige Skalierbarkeit und Flexibilität in der Verwaltung neuer aktueller Technologien sichert. So können große Mengen an Felddaten (Big Data) in Echtzeit archiviert, bearbeitet und analysiert werden, um damit Unternehmen zu ermöglichen, durch die Nutzung dieser Daten Mehrwerte zu generieren. Die Einführung von Cybersecurity-Richtlinien, wie der Norm IEC 62443, zwang den Kunden ebenfalls dazu, seine industriellen Netzwerkstandards neu zu überdenken.

Der Betrieb erforderte zudem eine Fernüberwachung und ein Teleservicesystem für die Anlagen, die gleichzeitig sowohl technische Interventionen der Hersteller als auch Sicherheit hinsichtlich Zugangskontrolle und Überwachung gewährleisten. Das Ziel war es, ein unkontrolliertes Zugangssystem, welches aus einem flachen Kommunikationsnetzwerk bestand, in ein Netzwerk umzuwandeln, welches am Ende des Projekts durch die Nutzung moderner Zugangsmethoden segmentiert und strukturiert ist.

Eine weitere Herausforderung bestand darin, Standzeiten zu vermeiden und somit Produktionsstillständen vorzubeugen, wie Andrea Di Nicola, Automation Manager bei Barilla in Rubbiano, erklärt: „Ein Kernelement dieses Projekts war die Implementierung der Teleservice-Infrastruktur von Siemens, basierend auf der Lösung SINEMA Remote Connect in Kombination mit der Firewall SCALANCE S. Der schwierigste Teil dabei war, die Netzwerkarchitektur während des laufenden Betriebs und in den kurzen Produktionspausen entsprechend umzustellen. Mit der Expertise von Siemens und seinem kompetenten Partner ITCore haben wir es geschafft, die Umstellung ohne jegliche Standzeiten durchzuführen – dank der sorgfältigen Steuerung des Produktionsbetriebs und der Netzwerkkonfigurationen, die die transparente und vollständig kontrollierte Übergangsphase möglich gemacht hat. Beide Unternehmen haben uns während aller Projektphasen unterstützt, vom Start bis zum abschließenden Training, dem technischen Bereich der Anlage und Wartung, sodass eine aufeinander abgestimmte Infrastruktur erschaffen wurde."



Die Produktion von Barilla profitiert vom neuen OT-Netzwerk.

Innovatives OT-Netzwerk erfüllt hohe Cybersecurity-Standards

Die Partnerschaft mit Siemens hat sich auf natürliche Weise ergeben, denn die Zusammenarbeit zwischen Barilla und Siemens erzielt schon seit Jahren hervorragende Ergebnisse. Dadurch entstand die starke Motivation, auf diese Weise weiterzumachen und Siemens anderen Automatisierungs-Unternehmen vorzuziehen: „Die vollumfängliche Zusammenarbeit mit Siemens von Anfang an war unser Trumpf, von der Voranalyse über die technische und wirtschaftliche Bewertung der Investition", erklärt Di Nicola. „Wir sind dieses Projekt gemeinsam angegangen. Die Grundidee war, die Welten von IT (information technology, Informationstechnologie) und OT (operational technology, Betriebstechnologie) miteinander kommunizieren zu lassen, da vor diesem Projekt das Automationsnetzwerk der Fabrik fast gänzlich im Bereich der IT von Barilla lag. Ziel dieses Projektes war es, die IT-Welt von der Automatisierungs-Welt zu trennen und sie gleichzeitig funktional zu verbinden."

Siemens hat Barilla zu diesem Zweck die innovativsten OT-Netzwerk- und Cybersecurity-Technologien empfohlen, die derzeit auf dem Markt erhältlich sind. Dadurch wurde die vollständige Kompatibilität der Geräte von Siemens mit Systemen und Komponenten anderer Automatisierungs-Hersteller sichergestellt.

Die Stärken lagen sowohl in den Komponenten und Kompetenzen von Siemens als auch in der Möglichkeit, durch herstellerunabhängige Kommunikation eine hohe Kontinuität des Produktionsprozesses zu garantieren.

Marcello Scalfi, Sales Specialist Team Leader Digital Connectivity and Power bei Siemens Italia, merkt an: „Die Integrationsarbeit zwischen den IT- und den OT-Teams, die von Siemens ausgeführt wurde, erforderte eine lange interne Evaluationsphase zusammen mit Barilla. Barilla zog mehrere Lösungen in Betracht, die wir in Trainings-Workshops vorgestellt haben. Diese richteten sich an die Kollegen in den Engineering- und OT-Abteilungen von Barilla und sollten ihre Networking- und Cybersecurity-Kompetenzen stärken. Mit dem Wissen um die verfügbaren Technologien konnten sie sich auch die nötigen Fähigkeiten aneignen, um die beste und praktikabelste Lösung zu erkennen. Für Siemens war es wichtig, eine Diskussion anzuregen und dem Kunden alle möglichen Szenarien darzulegen, sodass dieser eine bewusste Entscheidung treffen konnte. Diese wichtige Veränderung war eine lehrreiche Erfahrung für alle Beteiligten.

Neues Netzwerk soll Kontinuität der Produktion schützen

Das Projekt wurde von drei Beteiligten ausgeführt: Siemens, Barilla und ITCore.

ITCore ist ein Industrial Strength Network Partner von Siemens. In der Fabrik in Rubbiano hat das Unternehmen bei der Planung, Umsetzung und Wartung der gesamten Netzwerkinfrastruktur und des Teleservice-Systems eine zentrale Rolle übernommen.

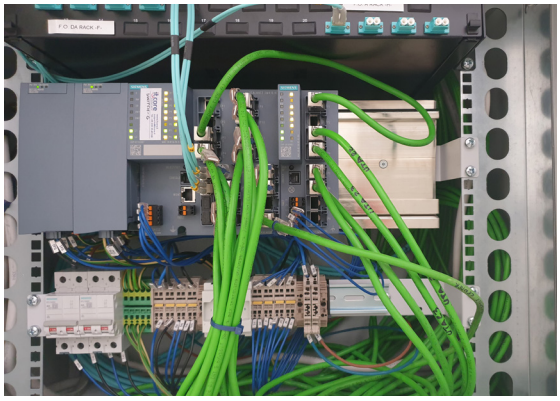
Das neue Netzwerk ist durch Regeln und Routing-Pläne strukturiert und hat mehr als 1.000 verknüpfte intelligente Knotenpunkte. Der Prozess sah die Schaffung eines Ring-Backbone-Netzwerks aus Glasfaser (auch genannt „Backbone") vor, das mit MRP (media redundancy protocol) gemanagt wird. Das Automatisierungsnetzwerk sollte mit VLAN (Virtual LAN) in Produktionszellen segmentiert werden.

Jede dieser Zellen ist netzwerktechnisch von den anderen getrennt und kommuniziert über die folgenden Geräte aus der Produktfamilie SCALANCE von Siemens:

- Industrial Firewall: Ein System für die Netzwerksicherheit, das ein- und ausgehenden Verkehr mit einer Serie vordefinierter Sicherheitsregeln überwacht und Events zulässt oder blockiert.
- Industrial Switches: Netzwerkgeräte, die für das Switchen auf dem Level der Datenverbindung zuständig sind. Bei mehreren verbundenen Knoten verwalten sie den Datenverkehr und trennen die sogenannten „collision domains", die an ihre Ports angebunden sind.

- Router: Elektronische Geräte, die Daten zwischen den Netzwerken routen und die Verbindung zwischen verschiedenen Terminals verteilen.

SCALANCE SC632: Die Ansammlung von Industrial Firewalls ermöglicht den korrekten Kommunikationspfad vom Anlagennetzwerk zur IT und umgekehrt.



SCALANCE XM416-4C: Der Kern des Produktions-Backbones, der dem Anlagennetzwerk Redundanz und hohe Verfügbarkeit verleiht.

Vervollständigt wird die Lösung von einem zentralen Management- und Kontrollsystem für Fernzugriff auf das Produktionsnetzwerk (Teleservice), das nach einem festgelegten „double jump host"-Modell integriert wurde. Die Implementierung der Lösung wurde ermöglicht durch die Funktionalität der Komponenten SCALANCE S von Siemens (Industrial Firewall), die den Zellen vorgeschaltet sind, sowie der Software SINEMA Remote Connect.

Networking und Cybersecurity im Industriesektor sind Themenfelder, mit denen sich ITCore, zusammen mit Siemens, täglich auseinandersetzt. „Wir glauben, dass in den nächsten Jahren die permanente Überwachung aller Geräte, die mit dem Netzwerk verbunden sind, unverzichtbar werden wird. Niemand wird die Digitalisierung aufhalten und wir müssen alles dafür tun, die Kontinuität der Produktion zu schützen, sowohl den funktionalen Betrieb als auch die generierten Daten", erklärt Federico Tarzia, Chief Technical Officer bei ITCore.

Resultate übertreffen Erwartungen

Die von Siemens implementierte Lösung erreicht die höchsten Cybersecurity- und Datensicherheits-Standards, die auf Ebene des Betriebsnetzwerks derzeit gültig sind. Das macht die Fabrik in Rubbiano zu einem Vorbild für die anderen Produktionsstätten von Barilla.

Neben der einfachen Wartung und dem Plug-&-Play-Austausch der Komponenten sowie der daraus resultierenden Reduzierung/Eliminierung von Stillstandszeiten durch Störungen war auch der Support ein zunehmend wichtiger Faktor, der es außerdem möglich macht, dass sich Barillas Investition vollständig amortisiert. „Mit der Ausbreitung der Pandemie auf der einen und der Notwendigkeit, die Produktion aufrecht zu erhalten, auf der anderen Seite, hat die Investition in eine zuverlässige Teleservice-Infrastruktur es uns durch Smart Working ermöglicht, auch dann „in factory" zu sein, wenn wir uns außerhalb befanden", bemerkt Di Nicola. „Gleichzeitig können Ausrüster, die aufgrund der Pandemie nicht für jede Änderung ins Werk kommen konnten, Teleservice nutzen, um auch in voneinander getrennten Umgebungen die Vertraulichkeit von Informationen zwischen zwei Lieferanten zu wahren." Die zeitgerechte Kontrolle dieses Zugangs und die Möglichkeit, Eingriffe von externen Lieferanten problemlos zu kontrollieren und zu verwalten war ein weiterer erfolgreicher Aspekt dieses Projekts.

Weitere Informationen

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts. Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter **www.siemens.de/industrialsecurity**

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Deutschland

Referenz
PDF 1121 5 De
Produced in Germany

Liste von Siemens Produkten

- SINEMA Remote Connect
- Router/Firewall SCALANCE SC600
- Router/Switch SCALANCE XR500
- Switch SCALANCE XM400
- Switch SCALANCE XC200

siemens.de/industrial-communication