



Improve the availability
and security of your plant
SIMATIC PCS 7 CPU 410 controller series

usa.siemens.com/v9

The flexible and powerful SIMATIC PCS 7 CPU 410 controller series is suitable for complex applications in the process industries. By incorporating the CPU 410 into your automation tasks, you are ensured not only the highest degree of availability, but also exceptionally reliable security against cyberthreats.

High performance

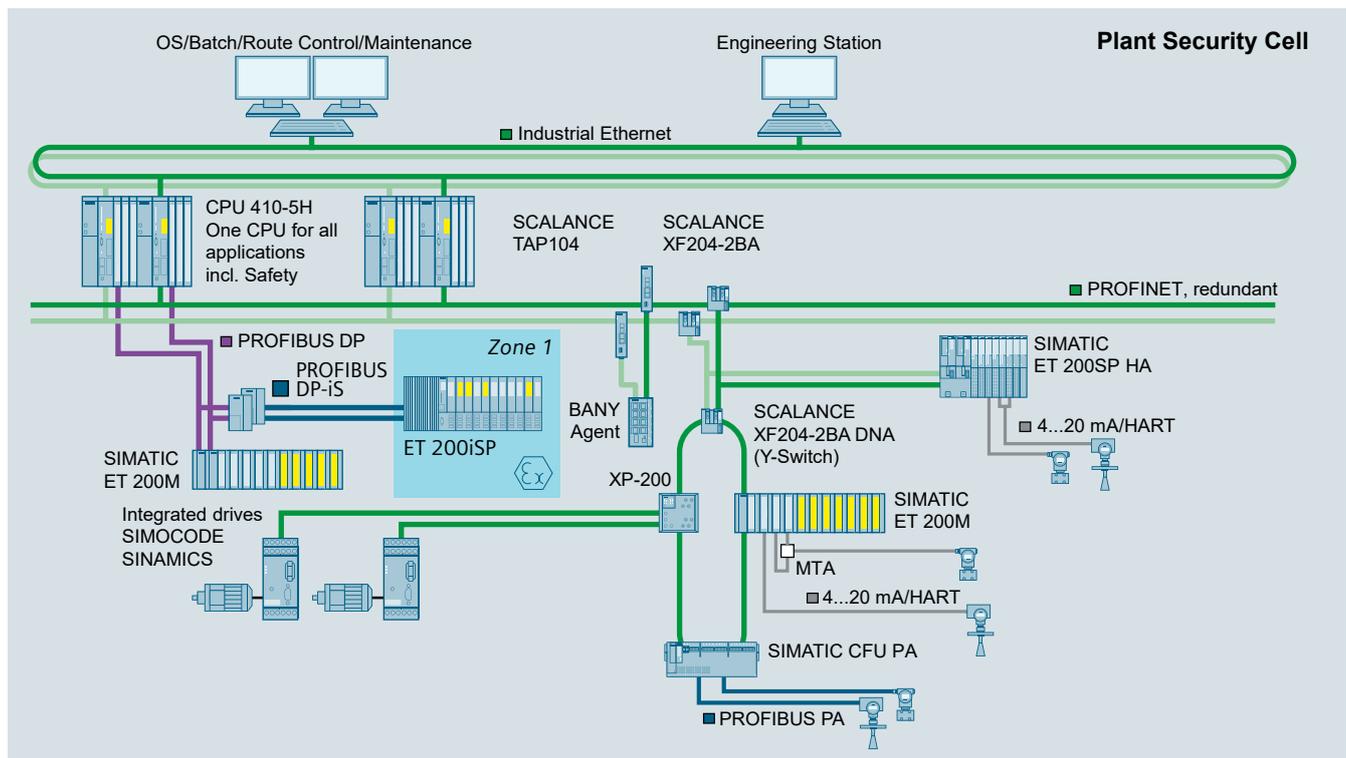
In the age of digitalization, the process industries are facing increasingly demanding challenges and dealing with sophisticated, complex applications. Due to its extensive scalability, the CPU 410 controller series offers the highest availability and multiple safety levels – making it the ideal controller for a broad range of applications.

Cybersecurity built in

Cybersecurity risks and appropriate defense measures are constantly changing. Stay ahead of the curve and keep your plant protected with the CPU 410, which has been designed and certified to meet the highest standards of security in process automation.



SIMATIC PCS 7 CPU 410: Highest standards of security in process automation



Security Information and Event Management (SIEM)

The CPU 410 logs all security-related events, including configuration and firmware changes, and automatically forwards them to a Security Information and Event Management (SIEM) server. This feature simplifies the process of collecting and reporting events across the control system architecture.

Field Interface Security

The CPU 410 also includes a Field Interface Security option for PROFIBUS DP and PROFINET. When activated, the CPU 410 becomes the only device capable of initiating communication with new devices added to the network – preventing any unauthorized changes from being made.

Certified for secure operation

The CPU 410 holds ACHILLES Level 2 certification for communication robustness. Additionally, Siemens is the first company to receive TÜV SÜD certification based on IEC 62443-4-1

Are you prepared for the next cyberattack?

Assets, equipment, uptime and personal safety need to be protected from malicious network intrusions, employee sabotage or accidental manipulation. To avoid damages and downtime from cyberthreats, it's important to implement an approach addressing the primary components of a successful security strategy: people, process and technology. To learn more, visit: usa.siemens.com/network-security

for the interdisciplinary process of developing automation and drive products, including the CPU 410. These robust, highly available and failsafe controllers were designed with a high focus on security.

The CPU 410 is an essential part of the SIMATIC PCS 7 distributed control system, which is certified by TÜV SÜD according to IEC 62443-3-3. The international standard IEC 62443 describes an IT security concept based on the deeply tiered "defense-in-depth" approach, in which device and system suppliers, system integrators and operators are involved and contribute toward the overall solution. On the basis of IEC 62443, companies can examine the potential weak points in their control system and develop effective protective measures.

Protect your programs and communications

With the CPU 410, you can apply security protections to the programs in the CPU down to the function block

level. It is also possible to encrypt all communications with the controller.

SIMATIC PCS 7 CPU 410 controllers: the right choice for high-performance, highly secure process automation!



Siemens Industry, Inc.
100 Technology Drive
Alpharetta, GA 30005
1-800-365-8766
info.us@siemens.com