openSAFETY meets OPC UA

Safe Line Automation

Industry 4.0 demands modular, flexible production lines. While these qualities are being implemented successfully at a functional control level, achieving comparable levels of flexibility in line-level safety technology has so far seemed an insurmountable hurdle. With the combination of OPC UA and openSAFETY, B&R aims to change that – providing seamless safety for production lines.

↓

"In theory it is certainly possible to join machines from different vendors in a single safety network," explains Franz Kaufleitner, product manager for integrated safety at B&R, "but doing so requires an extensive amount of factory-floor programming." Once the line is up and running, any time you add, remove or modify equipment, you would need to reprogram and recheck the safety application. "That's just not a viable solution in real-world conditions," says Kaufleitner.
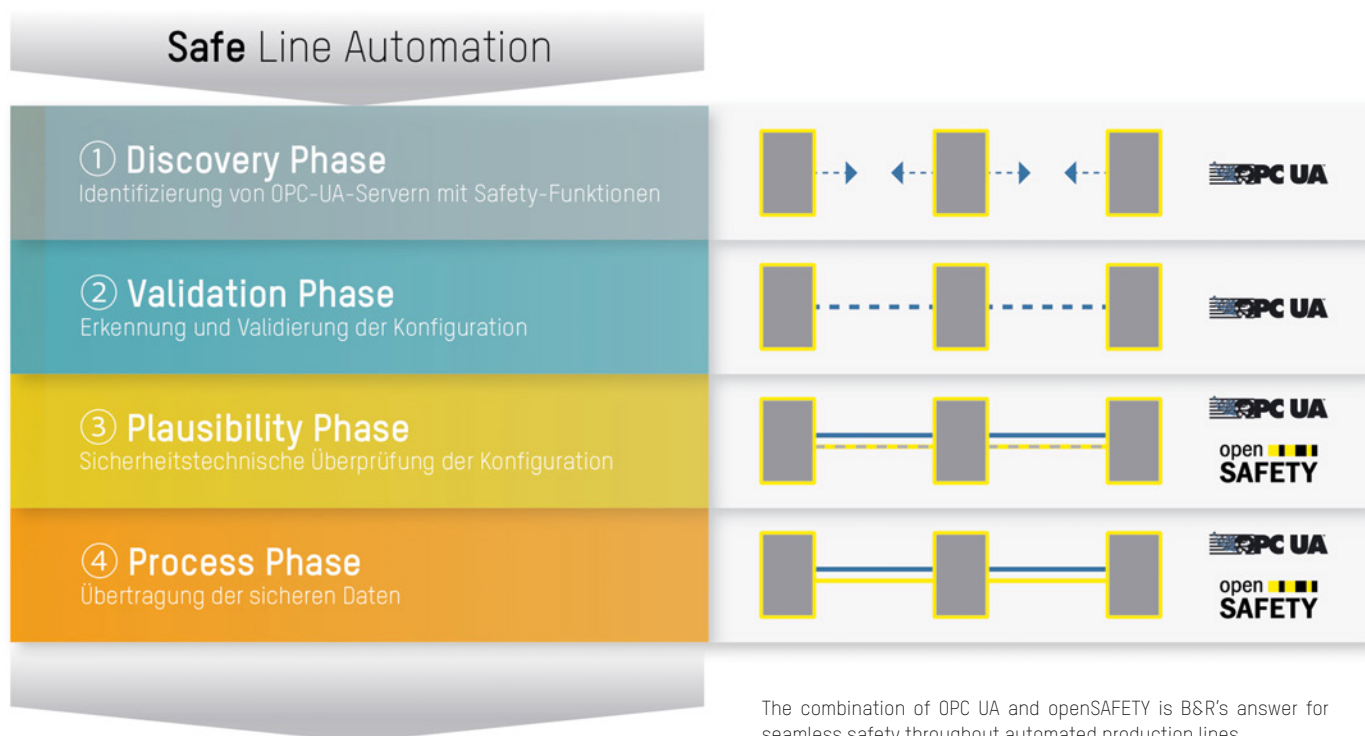
High level of flexibility required

That's why B&R is working on a concept that will open up a whole new realm of solutions: self-organizing safety networks based on OPC UA and the open source safety protocol openSAFETY. This technology will make it p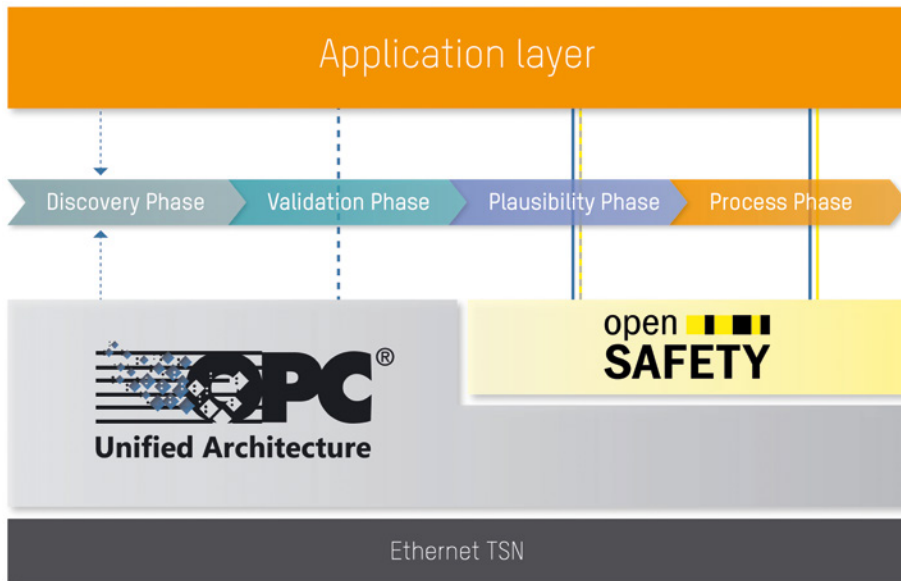ossible to add or remove entire machines or individual components from the machine network without having to reprogram the safety application. "It would even be conceivable to create a self-validating line," says Kaufleitner.

To allow the safety network to self-organize – while continuing to meet all the requirements for safety and security – there are a number of measures that need to be implemented. "This is where the particular advantages of OPC UA and openSAFETY really come to bear."

How it works

When a new piece of equipment – be it an entire machine, an individual part or even a robot – is added to the machine network, OPC UA security mechanisms begin by establishing a secure connection.

The combination of OPC UA and openSAFETY is B&R's answer for seamless safety throughout automated production lines.

Application layer

Discovery Phase → Validation Phase → Plausibility Phase → Process Phase

OPC® Unified Architecture

open SAFETY

Ethernet TSN

openSAFETY exchanges data using the OPC UA publish-subscribe model.

Then the OPC UA discovery service and server capability identifiers are used to search for servers that offer safety functions, after which OPC UA browsing services identify the functions and corresponding attributes available on each server. In this way, any OPC UA server is able to obtain a complete map of the network without requiring a single line of code to be written. "This process can already be implemented using OPC UA," notes Kaufleitner.

Automatic check

Next, the safety application checks whether the new component is already known, or if – with regard to safety – it matches a previ-ously validated configuration. If so, there is nothing else for the machine operator to do.

If significant differences are identified, the user is asked to confirm via the HMI application whether the new configuration is correct. This input is saved, so the next time the same configuration will be recognized automatically.

Testing response times

"This is where openSAFETY comes into play," explains Kaufleitner. Each component checks the plausibility of the configuration. "This process is the same as the checks that are generally performed when a machine is started up." This includes a test of whether the response times and cycle times are fast enough to ensure reliable execution of the respective safety functions. Once these checks have been completed, exchange of safety-relevant process data via openSAFETY begins and the production line can resume operation.

Devices react automatically

As a minimum requirement for implementing safe line automation, each device needs to support openSAFETY's E-stop profile. If an E-stop button is pressed, all devices in the openSAFETY network are notified automatically. Each of them decides independently whether to enter an E-stop state or if it's possible to continue running. "This would be the case, for instance, if the event affected a different E-stop zone."

A linear profile is currently in development that will allow individual components of the machine or line to communicate directly with their neighbors. If one machine component enters a safe state, its immediate neighbors decide autonomously whether they need to enter a safe state as well, or if they are able to continue running, possibly at reduced speed. "All the components, throughout the entire line, communicate with each other without any intervention from a higher-level system or operator," says Kaufleitner. ←

open SAFETY

How does openSAFETY communicate via OPC UA?
The open source safety protocol openSAFETY can use any fieldbus or Industrial Ethernet network as its transport medium. The black channel principle ensures that openSAFETY data is transported completely independently of other traffic.

openSAFETY exchanges data using the OPC UA publish-subscribe model. As a result, openSAFETY nodes can communicate with each other directly and achieve extremely fast response times. Additionally, OPC UA method-calling functionality is used transfer openSAFETY data via OPC UA in order to check the plausibility of the safety application.