versiondog Factsheet:

versiondog switch integration – the honeypot scenario

versiondog – providing the automation industry with more certainty, safety and security

versiondog is the leading version control and data management software for automated production. It makes tracking changes and safeguarding data significantly more efficient.

versiondog brings order and clarity where project data needs to be continually changed and made available from a central source. The increased safety, security and certainty provided by this software system quickly results in measurably increased productivity.

Furthermore, versiondog makes it easy for you to optimise the interplay between all your different types of robots, controllers, field devices, drives, programming languages, file formats and software applications.

This data management system gives you ultimate data traceability and data availability, minimising your risks and costs, and saving you time and effort.

Data management as part of your cybersecurity strategy

Cybersecurity is one of the central topics in industrial automation. Although versiondog does not directly repel cyberattacks, it helps customers to detect them early on. And, very importantly, it can significantly reduce the damage wrought by a cyberattack by quickly restoring the last unchanged, hence virus-free version.

In order to detect cyberattacks early on, it is essential that you are able to track changes to all control programs and production data. It is also imperative that you are able to identify any unauthorised program changes immediately. All of this is possible with AUVESY's data management and software solution, versiondog. With versiondog, you can quickly see WHO changed WHAT, WHERE, WHEN and WHY (from the current version all the way back to the first version). What is more, a configurable alarm alerts you when discrepancies are found.

If a cyberattack has already taken place, the fastest solution is to quickly find and restore a previous, virus-free version. It stands to reason that if you make regular backups you reduce the likelihood of data loss. Regular backups also allow you to perform rapid restoration, whereby maintenance staff can take an error-free backup from the server archive and immediately restore it. This process is also known as disaster recovery. In the versiondog world, disaster recovery is made much faster thanks to the data management and software solution's ability to schedule automatic backups and to precisely compare versions with SmartCompare. versiondog's ability to restore a previous, virus-free version of an automation device, and thereby return it to the state that it was in before the cyberattack, prove that versiondog has the potential to function as part of an effective cybersecurity strategy and that it should be incorporated among the diverse range of other defensive strategies that make up any company's defence in depth strategy as a whole.

The honeypot scenario

Industrial networks are very complex. They are often structured into several hierarchical levels and have a clearly defined communication protocol so as to successfully facilitate the management of data streams and tasks. At the field or machine level, there are switches which are connected to terminal equipment (such as controllers, field devices and HMI panels) via an Industrial Ethernet protocol (e.g. PROFINET). Switches frequently account for the earliest targets of a cyberattack due to their ability to access automation devices via ports. If a port is opened or closed as a direct result of a cyberattack, the connection to the terminal device can be severed or unauthorised access to a device can be granted. Both of these outcomes can put enterprises, persons and the environment at great risk. How does one go about preventing them?

One well-known example of a successful defence in depth strategy is the honeypot. Honeypots are used to detect (early threat detection and new threat detection), prevent, deflect and counteract malware. One way of doing this involves installing and configuring a switch in an industrial network. The honeypot (in the context of this scenario, a switch) has no real function, it only mimics the behaviour of a production resource as accurately as possible so as to appear attractive to unauthorised entities. The honeypot administrator should not make any changes to the switch, but simply monitor it for any unauthorised changes.
Enter versiondog. versiondog checks whether there were unauthorised changes made and sounds an alarm when discrepancies are found. This then allows for authorised personnel to react and prevent the potential consequences of a cyberattack. By using versiondog to schedule regular, automatic backups, you are able to monitor the configuration data of the switch and immediately detect unauthorised changes.

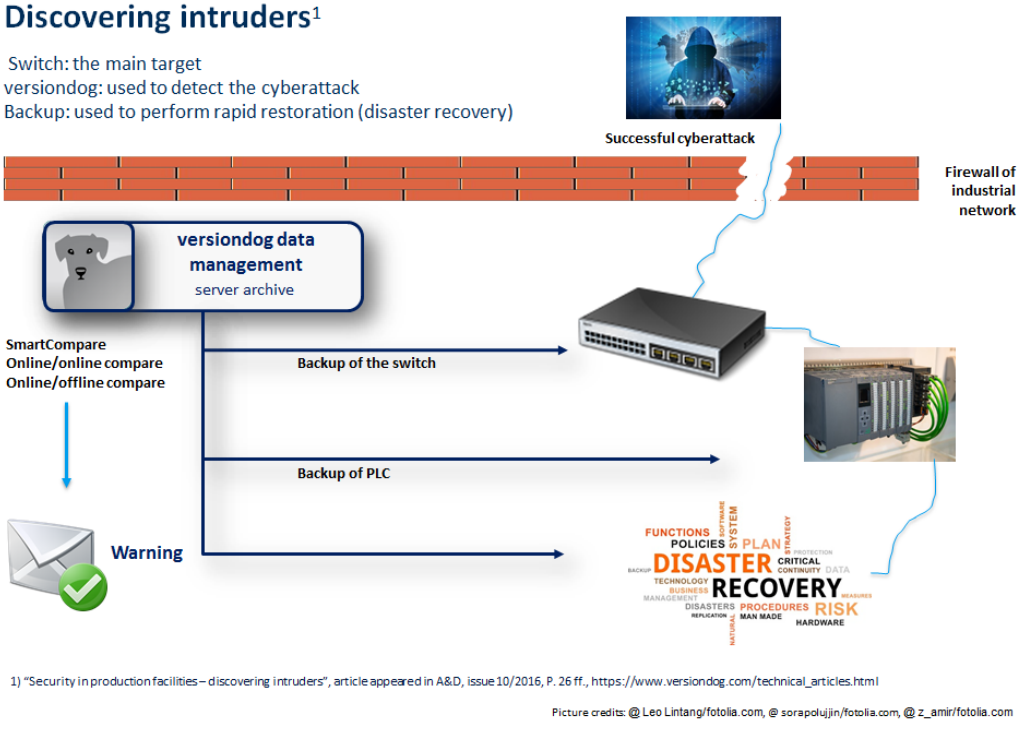


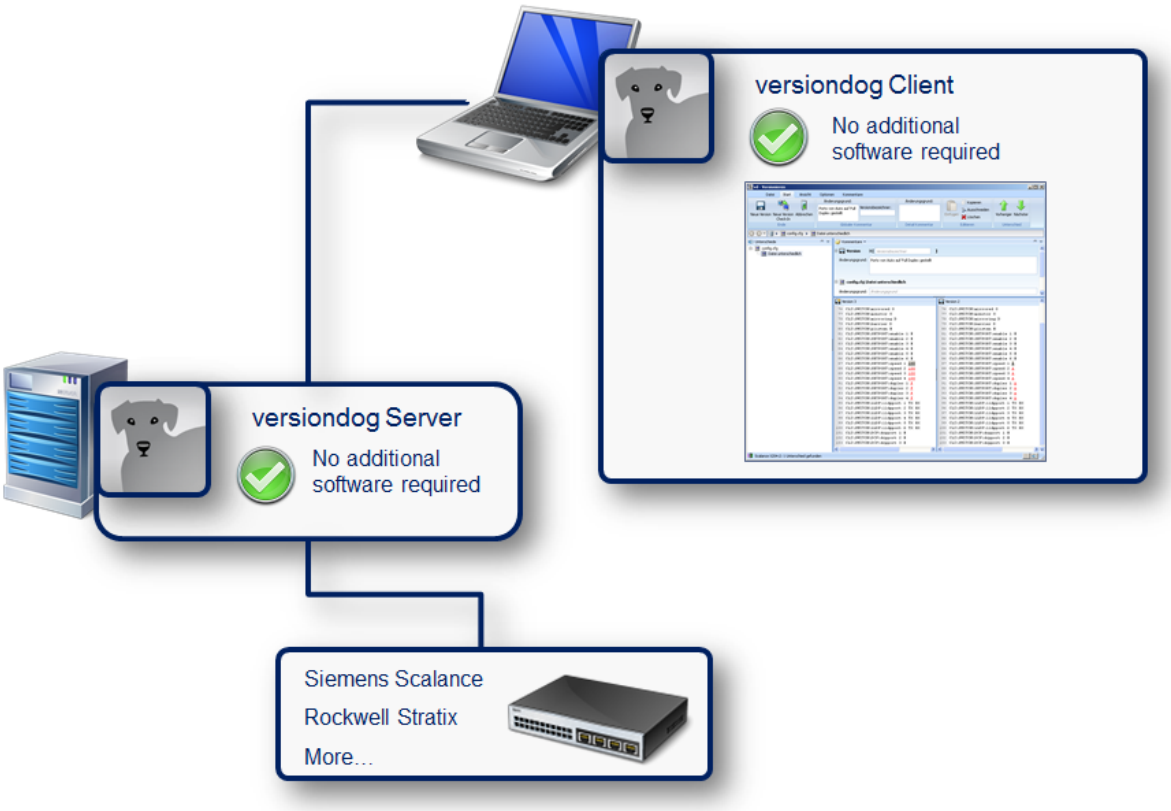
Figure 1: Honeypot scenario. A switch in an industrial network, to which no changes to the program code will be made, will be monitored by versiondog for any unauthorised changes. If during a routine data comparison, unauthorised changes are detected, versiondog will immediately inform the system administrator.

AUVESY.

versiondog switch integration

How does versiondog help you to safeguard your data?

- versiondog allows you to cyclically and automatically verify authorised control program versions
  - ✓ Perform multiple checks daily
  - ✓ Get alarm notifications
  - ✓ Quickly comprehend differences through text-based and/or graphical display
  - ✓ Suitable for use with the vast majority of automation devices and systems
- versiondog detects changes to control programs and displays them
- versiondog monitors the system configuration of Windows and Linux based systems
- versiondog ensures that versions cannot be subsequently changed
- versiondog quickly finds and restores a previous, error-free version



AUVESY.

versiondog switch integration

Main features and functions

Automatic backup, version control, documentation and change management for software projects	✓
SmartCompare for all components in automated production	✓
Online/online and online/offline comparisons	✓
Data organised with 100% clarity and traceability	✓
See WHO changed WHAT, WHEN, WHERE and WHY	✓
Configurable alarm for when discrepancies are found	✓
Fast and reliable disaster recovery	✓

System requirements

versiondog version	from 5.0 onwards

More information

AUVESY GmbH
Tel: +49 (0)6341 6810-440
Email: info@versiondog.de
Web: www.versiondog.com