Extract from the White Paper „Web Technology in Automation“

Important security aspects for using Saia PCD® controllers and HMI conntected to Internet/LAN

First Edition: 2007

Security

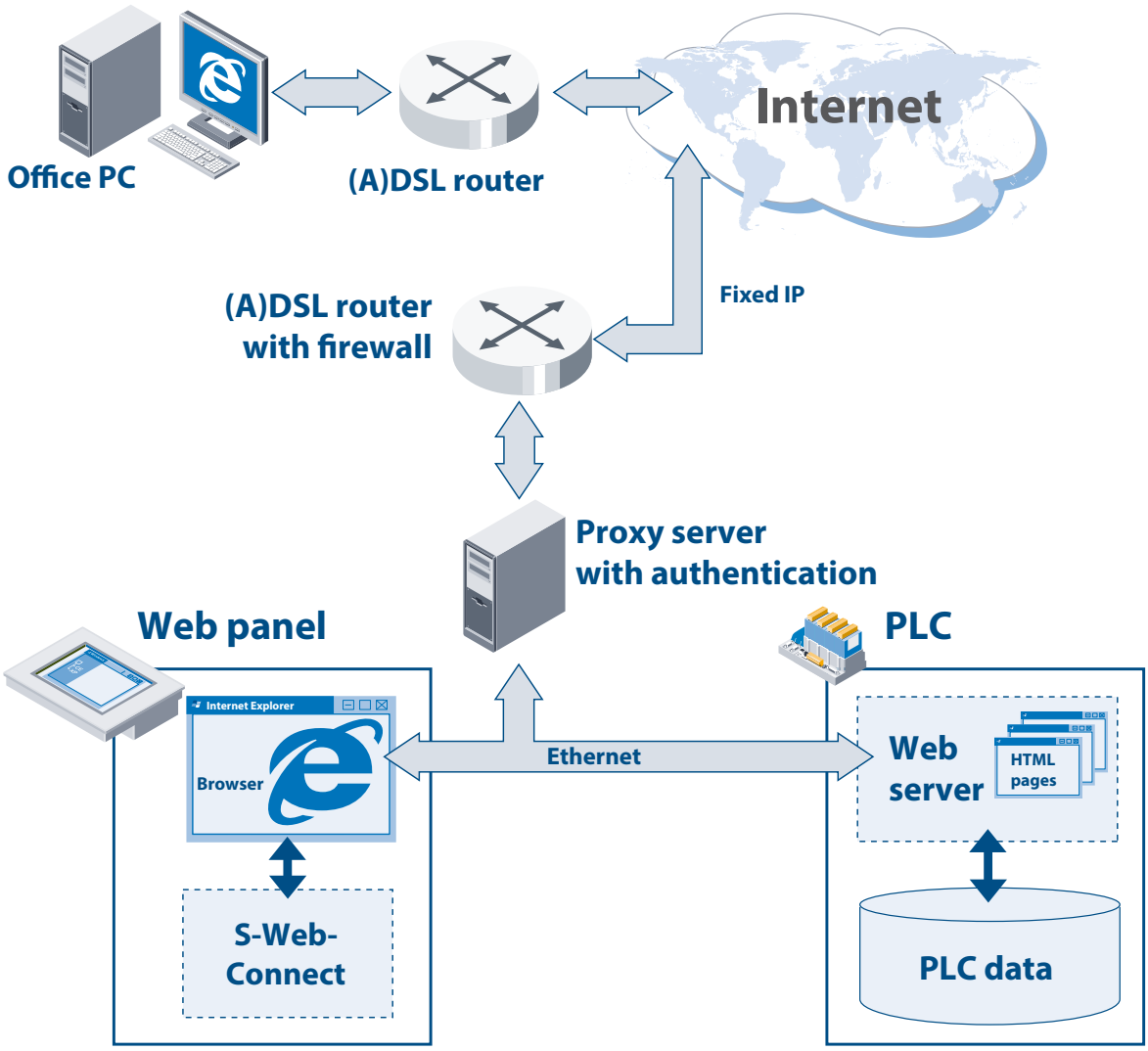
When discussing web technology, sooner or later the subject of security is raised. Hardly a day goes by without someone trying to convince us our Windows® PCs are supposedly insecure. In the meantime, a whole industry has grown up around the fear of attack from hackers or viruses. This is not to say that the subject of security should not be taken seriously, but instead that it could benefit from more objective, sober consideration.

Microsoft® does indeed have a problem with security: the matter has been looked after carelessly. However, an operating system is the worst place imaginable to construct effective protection. This is due not only to the complexity of today's operating systems, but also to the fact that it is hard to believe in effective protection when the intruder has already reached the computer. In professional settings, therefore, the subject of security is approached separately from the individual work station (i.e. the individual PC). Dedicated components exist for this purpose and provide a stand-alone protective function, e.g. HW firewalls. In fact, most (A)DSL routers include a firewall, the effectiveness of which is preferable every time to a SW firewall installed on a PC. Transferred to automation technology therefore, it would be inadvisable only to seek to implement security in the controller. Instead, the environment in which controllers and web panels are used should be built securely.

In general, security in IT applications can be divided into two subject areas: unauthorized penetration of computer and network systems (hacking) and viruses. Viruses rely on HW platforms with the widest possible distribution and standard operating systems, such as Windows® PCs. As a rule, controllers are built with optimized microcontrollers or processors and equipped with a proprietary operating system. This makes them immune to all viruses written for PCs and Windows®. Compared to PCs, the restricted distribution of controllers makes it highly improbable that special viruses for controller systems might turn up. Theoretically, Windows®-based control panels would be more susceptible. Developers of viruses want to achieve the greatest possible effect and therefore target the desktop operating systems: Windows® 2000/XP/Vista. Even Windows® CE is already much less attractive. It should also be noted that viruses are mainly introduced and activated by the user. This can happen quickly with one click too many when surfing on internet, or by installing an infected program. Control panels in industrial applications are usually closed, i.e. an operator interface starts up immediately when the machine boots up and the operator has no opportunity to drive critical web pages or even install software. With Windows® XP-based panels in particular, anyone who wants to play safe can install a virus scanner. However, in this case a scanner should be chosen that is automatically updated with the latest virus signatures and does its job discreetly in the background, without annoying pop-up

windows® or forced user interaction. Unfortunately, most commercial virus scanners fail on this point. This does not have to be the case, as the company Eset® (www.eset.com) has demonstrated with its product Nod32. Nod32 is capable of running with absolutely no user interaction in so-called «silent mode» and even sends emails when any infection is detected.

Compared with the risk from viruses, considerably more importance should be attached to hacking in industrial applications. Sturdy access control is particularly necessary for web visualization systems whose entire user interface is delivered free to your door, so to speak. This can be achieved by the forward switching of a proxy server with authentication. Queries received via internet will first be channelled to the proxy server. Before the proxy server forwards any query to the appropriate controller, the user must log on with a user/password code (authentication). This ensures that only a specific group of persons will have access. If you also want to protect yourself against «sniffer» attacks, the proxy server can provide SSL encryption of all data traffic. This allows you to achieve the same security level as web shops and online banking. Another access control method is the VPN (virtual private network). This transmits private data across the internet in a so-called tunnel. Transmission can be encrypted. With a VPN tunnel, users can access computers via internet in the same way as if they were located in a LAN. To access a VPN, a software client must be installed on the computer (PC), which then establishes the connection. It is not absolutely necessary to use a full-blown server PC before you can enjoy the security techniques described above. Compact devices are available on the market that have been specially designed for insertion in the control cabinet. For example, the company Eurogard (http://www.eurogard.de/eurogard_e.htm) offers an economical service router with proxy server, SSL encryption and VPN, geared specifically to PCD controllers from Saia-Burgess Controls.



Access to internet protected by Proxy-Server for web panels and controllers

Saia-Burgess Controls AG
Bahnhofstrasse 18 | 3280 Murten, Schweiz
T +41 26 672 72 72 | F +41 26 672 74 99
www.saia-pcd.com

support@saia-pcd.com | www.sbc-support.com

P+P26/261 EN03 02. 2014 Subjects to change without notice.