Strictly no admittance

Keeping an eye on IT security in the plant

Markus Brändle, Thomas E. Koch, Martin Naedele, Rolf Vahldieck

Electronic attacks on the automation systems of industrial and utility plants are rare. Nevertheless, when they do occur, the consequences can be severe.

Strategies used to protect office networks (for example) are not always directly applicable to the specific needs of industrial and utility plants. Whereas traffic on an office network is largely arbitrary from a monitoring point of view, and intrusion detection is often restricted to scanning data packets for specific attributes, network traffic in a plant is normally easy to correlate to the system's activity. Significant deviations from expected patterns can be an indicator of intrusions. ABB's System 800xA Security Workplace uses this to add security functionality to System 800xA control systems. Because the approach builds on proven System 800xA concepts, operators do not require special IT-security training to be able to make good use of this tool.

In view of the continuous evolution in the capabilities of computers, and also the multiplicity of means of access (network connections, modems, memory sticks, CDs, laptops, etc), it is no surprise that new vulnerabilities are continually being discovered and exploited. No security mechanism can guarantee absolute invulnerability against attacks and intrusions. A polyvalent security architecture therefore relies not only on preventive mechanisms such as firewalls and antivirus tools, but also includes technology and process elements to detect ongoing attacks and intrusions and is able to react to them.

One option for such detection capability is a dedicated team of humans that monitors and analyzes intrusions. Operating such a team around the clock implies a significant and continuous financial investment, which may be hard to justify. Moreover, attracting and retaining qualified team members can prove difficult in an environment that only very rarely encounters an actual attack.

A more cost-efficient alternative for a plant would be to subscribe to the services of a managed security service provider, using central monitoring facilities with highly qualified staff to continuously and concurrently monitor the networks of multiple clients. While significantly less costly than the in-house equivalent, the external service provider approach may still be too costly for low risk plants. Furthermore, there are other concerns that may make this approach unsuitable: These can be related to security, (external access would have to be provided) or to safety (can the external service provider be trusted to properly appreciate the peculiarities of industrial plants and the related hazards?).

For these situations, ABB offers a third alternative – the integration of IT security monitoring in the overall process control structure.

Process operators, thanks to their training and everyday work experience in monitoring hundreds of process indicators, are very good at detecting anomalies in values and their correlations.

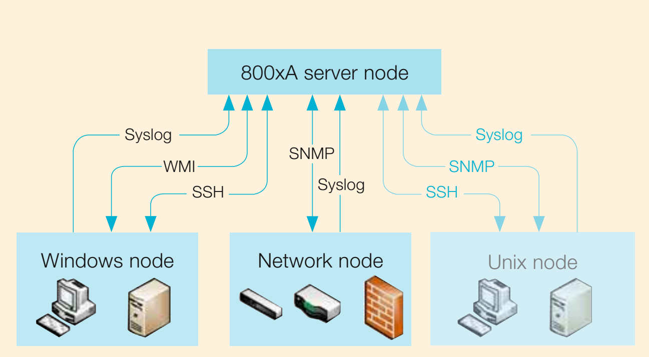
Security monitoring and process control

Many companies have technical attack detection capabilities, such as network-based intrusion detection systems, host-based intrusion detection systems, or scanners analyzing log messages from firewalls and hosts. However, many of these companies don't make effective use of these technical capabilities because they lack the staff resources to monitor the output of such tools around the clock.

Whereas IT security for automation systems has to overcome a number of specific challenges, some of them differing from those faced in IT security in offices [1], it also has certain advantages: One of these is that, very often, a process operator is available to monitor system behavior at all times. The availability of the process operator suggests that ideally he should also act as a kind of "first responder" with regard to IT security.

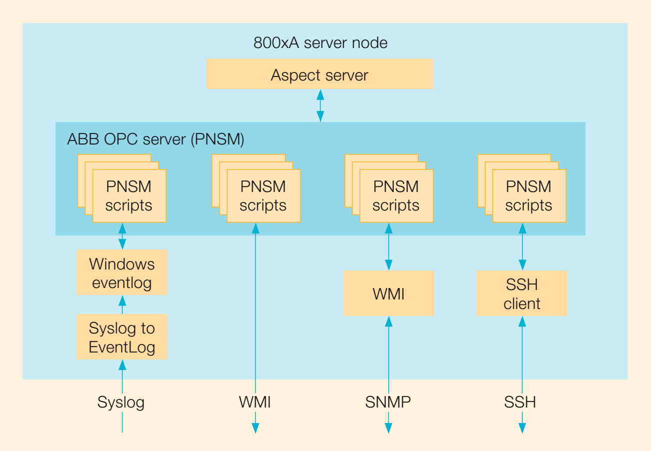
One objection to this approach may be that such a first responder role would require IT and IT-security knowledge, which is often not found among process operation staff. This lack of expertise is being addressed through increased automation of the analysis and detection function using complex rule-bases [2]. The removal of the human with his lack of expertise from the loop permits the derivation of fast and deterministic decisions providing clear responses in clear situations. Many real-life situations are, however, ambiguous: The environment is too dynamic for a fixed attack detection rule-base, and an approach based on dynamic updating of the rule-base would bring back the requirement for continuously available experts. ABB's approach, in contrast, is that process operators, thanks to their training and everyday work experience in monitoring hundreds of process indicators, are very good at detecting anomalies in values and their correlations. These people can use common sense to decide whether there is an uncritical explanation for anomalies – both in control parameters and in security-related areas.

1 Data flow for the System 800xA Security Workplace. Network traffic data is collected from various nodes and analyzed for anomalous behavior.

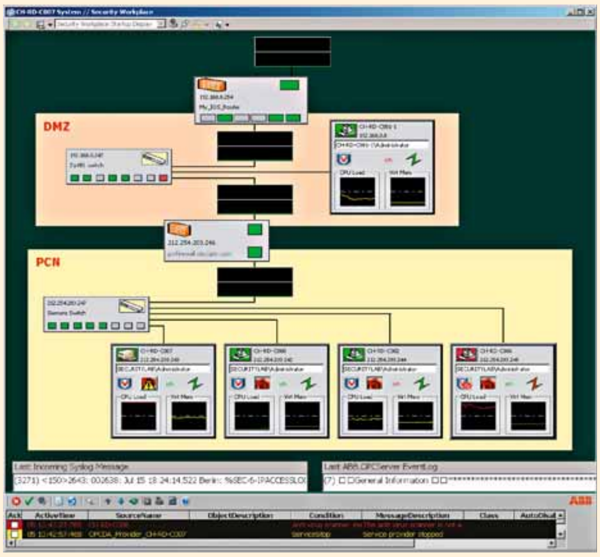


A more detailed view of the server node is shown in 2.

2 Overview of the architecture of the 800xA Server with Security Workplace



3 800xA Security Workplace showing the overview of the IT network



For example: A visualization of the hosts in the automation network displays the number of logged-in users. In the process operator's experience over past weeks, this number is constant. It is not necessary for him to know that the actual value results from logged-in human users (on some hosts) and service accounts for certain applications. Suddenly, he observes that on one host the user count is one higher than normal. Typically, this would be a highly critical sign of host compromise, indicating that an attacker has broken into a user account. In this specific case, however, the processor operator can easily correlate the initial appearance of the additional user on his monitoring system with the fact that a technician has recently entered the control room to effect engineering work. This type of plausibility check is essentially impossible to codify in a fully automated system and the corresponding false alarms are among the main reasons of the poor reputation automated intrusion detection systems have [3].

ABB's vision is to provide the process operator with the tools and methods to deal with plant IT security problems similar to process deviations [4]. The realization of this vision depends on the following prerequisites:

- IT security related information has to be presented to the process operator as part of his normal process-related work environment.
- IT security related information has to be presented to the process operator using the same presentation paradigms he is used to from process monitoring. This includes process graphics, colors, symbols, figures, and trend charts, and excludes messages containing cryptic "hacker terminology".
- The process operator should not need any specific IT or IT-security knowledge in order to detect an attack and react to it in a meaningful way. Possible reactions could include isolating the automation system from external connections, activating predefined network islands inside the automation system, starting a vulnerability check, collecting additional data according to predefined procedures, or calling for expert help.

Starting from these requirements, ABB has developed a security and system health monitoring and visualization solution for process control systems based on the System 800xA framework – System 800xA Security Workplace.

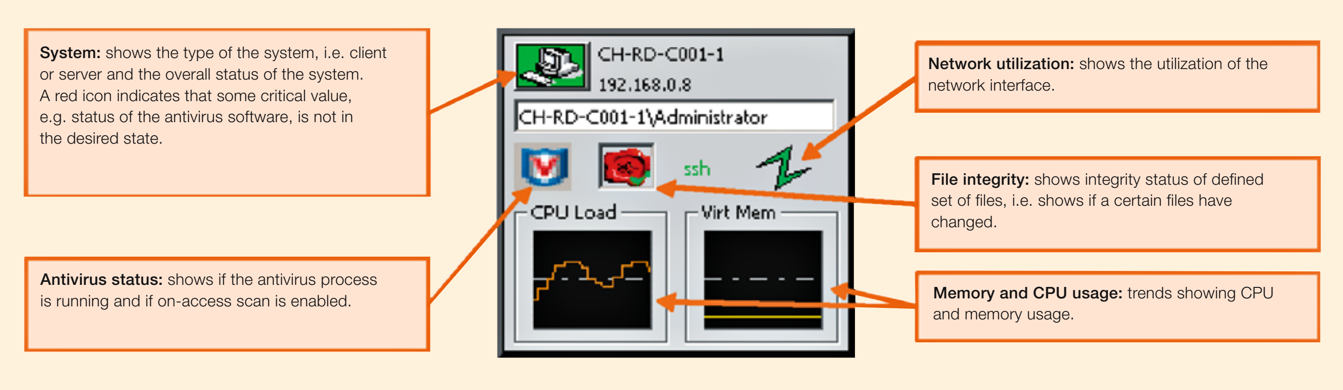
System 800xA Security Workplace

System architecture

System 800xA Security workplace consists of several faceplates and scripts that are loaded into the System 800xA at runtime. The security workplace thus uses and builds upon the 800xA base libraries and framework, illustrating how the high flexibility and straightforward integration capabilities of the 800xA architecture can be extended to such specific purposes as security monitoring.

The 800xA Security Workplace incorporates data from different sources and accessed by different technologies. 1 shows a high level overview of the systems involved and the data flows between them. The current prototype collects data from Windows nodes using Syslog messages, Windows Management Instrumentation (WMI). Data from network nodes (eg, firewalls, switches, or routers) is accessed using Simple Network Management Protocol (SNMP) and Syslog messaging. The current product extension does not include Unix nodes. However, accessing data from Unix nodes is simple using SNMP, SSH, or Syslog messaging.

4 The icon (from 3) showing the status of a computer system in the network



System: shows the type of the system, i.e. client or server and the overall status of the system. A red icon indicates that some critical value, e.g. status of the antivirus software, is not in the desired state.

Antivirus status: shows if the antivirus process is running and if on-access scan is enabled.

Network utilization: shows the utilization of the network interface.

File integrity: shows integrity status of defined set of files, i.e. shows if a certain files have changed.

Memory and CPU usage: trends showing CPU and memory usage.

The architecture of the 800xA server node needed to access the data from the different sources is shown in 2. The data is accessed using a System 800xA PC, Network and Software Monitoring (PNSM) scripts and provide the interfaces to connect to the various data sources[1].

PNSM (PC, Network, Software Monitoring), which is used as the backbone of the security workplace, is a set of 800xA features for monitoring the hosts and network elements in an automation network. PNSM provides a pre-configured library of IT Assets representing devices and system processes widely used within industrial businesses today. Through PNSM, Security Workplace incorporates data from the complete IT system: data from network devices such as firewalls and switches, from network segments and from computer systems attached to the network. The data collected consists of general IT data, such as CPU load, and security specific data, such as information on antivirus installation. Some of these more security related IT assets and information sources were added for Security Workplace.

Overall, the easy integration of information sources and the increasing autonomous behavior of components will lead to the implementation of fully automated and secured plant management. [5].

Operator perspective

Security Workplace is tailored to be used by a “normal” 800xA operator, ie, a person who does not necessarily have an IT-security background and in-depth knowledge of IT networks and systems. The data displayed should therefore not require skilled interpretation – Security Workplace must be capable of highlighting signs of possible attacks. It is not the intention that the operator should be able to identify the type of attack precisely or to react to possible attacks from within the framework of Security Workplace.

The look and feel of Security Workplace resembles a standard 800xA workplace. It contains standard elements such as faceplates, trend displays or alarm lists. Having this seamless integration into the well known working environment fosters acceptance by the operators and does not introduce the additional complexity of a new user interface that a dedicated security monitoring software from an external supplier would introduce.

3 shows the Security Workplace for a demonstration system. It consists of a process control network (PCN), a demilitarized zone (DMZ) and an external insecure network (eg, the Internet or business network). These zones are separated by firewalls and the PCN and DMZ have managed switches to connect the different nodes. The DMZ holds a proxy server that allows the PCN to be connected to from the outside. The PCN holds four different windows systems, an 800xA Aspect server, and 800xA Aspect Optimization server, a Windows Domain server and an 800xA Operator Workplace.

The depiction of the IT system within the Security Workplace resembles the actual physical setup. This will make it easier for the operator to understand what he is looking at. In case of larger systems, which cannot fit onto a single screen, the network can, as is common for complex process pictures, be displayed at different levels of detail on different displays.

For Microsoft Windows-based systems, the workplace overview of the 800xA Security Workplace depicts a summary of the health of the system. 4 shows such a system icon explaining the most important information depicted in the icon.

The overview of the 800xA Security Workplace also contains icons for all network devices. It shows basic information for the devices, ie, type of the network device, IP address, name, and status of the ports. 5 shows icons for a firewall (left) and a router with firewall capabilities (right). The firewall has two ports that are both connected, the router has one port connected to the outside network and six ports connected to the inside network. The icon shows that out of the six ports facing inside, three are connected. The colors of the ports indicate their status, green for correctly connected ports, grey for correctly unconnected ports and red for misconfigured ports, ie, ports that are connected but should not be connected or vice versa.

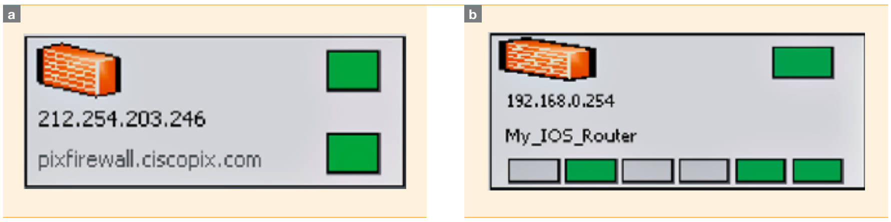
The security workplace also shows information on the network usage on various links. Small trend displays show eg, the amount of data received and sent by a network device or the number of packets received that were discarded 6.

All icons shown in the overview are linked to faceplates offering more extensive information. For network devices, the faceplates show the network usage of all interfaces individually and contain detailed trends for each interface showing the number of

Footnote

[1] The different methods of accessing the data are described in detail in technical documentation

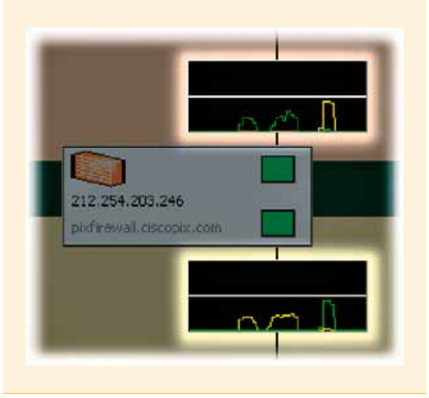
5 Icons representing firewalls and their statuses, as displayed within the network overview 3



212.254.203.246
pixfirewall.ciscopix.com

192.168.0.254
My_IOS_Router

6 Icons showing network loads (green is data received, yellow is data sent)



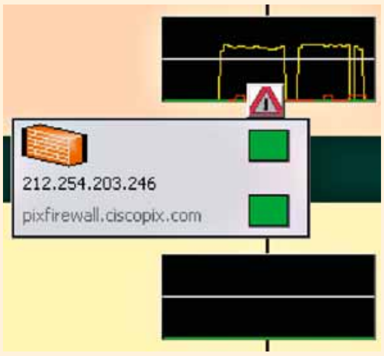
212.254.203.246
pixfirewall.ciscopix.com

packets received, the number of packets sent, the number of dropped packets, the number of erroneous packets etc. For Microsoft Windows systems the faceplates contain detailed information on the operating system (eg, version, installed service pack), the active sessions, the status of running threads, and trends on CPU usage, memory usage and thread activity.

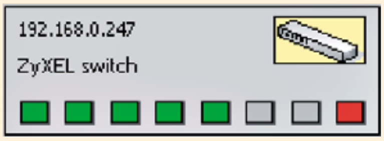
Example of detection of irregularity

As mentioned above, Security Workplace was designed to detect signs of attacks and to alert the operator. An important part of detecting attacks is first defining a "normal" system state. The workplace allows the definition of thresholds for various values that, when exceeded, will trigger an alarm. In this respect the arrangement is similar to standard process supervision. In contrast to other intrusion detection system (IDS) approaches, however, thresholds are not predefined but it is up to the operator to decide what is normal and what is not.

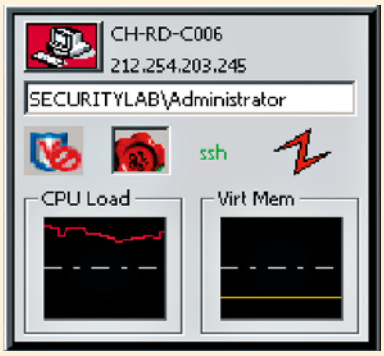
7 Possible attack on a firewall



8 A switch icon showing an illegal port use (red)



9 A Windows system icon with antivirus turned off



Network loads, for instance, are constantly monitored; a sudden increase of network traffic will result in an alert. Deviations from normal network loads can be a sign for a security incident, eg, network scanning or a malware trying to send data. 7 shows a scenario in which network traffic seen at a firewall is abnormal and one-sided, ie, traffic is only arriving at the firewall and not being re-transmitted. In addition, the network load has crossed the threshold (indicated by the exclamation sign) and some of the packets are erroneous (indicated by the red data plot). The fact that almost no traffic is sent from the firewall on either interface suggests that someone is either scanning the firewall or trying to send data to the PCN that is blocked by the firewall. Both would be a clear sign of an attack. Alternatively, it could be that a technician is uploading a file onto the firewall, eg, a new firmware, causing the abnormal traffic load. However, the high number of erroneous packets makes this unlikely.

Whereas the information shown in 7 gives indications on the type of attack, it is still unclear where the attack is originating from. This information has to be found elsewhere in Security Workplace: 8 shows the network switch residing in the DMZ that is also connected to the outside interface of the firewall. Shortly before the attack the rightmost port in the graphic started to blink in red. This means that a device, eg, a laptop, has been connected to this physical port even though the port should not be connected to anything.

The correlation of the information and the fact that the operator knows that a technician is performing maintenance of the DMZ network allows the operator to assume that the irregularity is caused by the technician's laptop. It can either be that the technician is actually performing a firmware update of the firewall or that the technicians' laptop is infected with eg, a worm that is trying to spread through the firewall.

A different scenario is shown in 9. The monitored Windows system has its antivirus functions turned off and the CPU load is very high. The disabled antivirus software would have triggered an alarm. Similarly to the previous scenario the operator might have additional knowledge to understand the event, eg, someone doing a software update on that machine. However, the antivirus software should typically never be disabled and this scenario would thus have to be classified as a security incident regardless of the circumstances.

The System 800xA Security Workplace and associated integration services are available from ABB Consult^{IT} Security Consulting Services. Contact Rolf Vahldieck (rolf.vahldieck@ch.abb.com) or the other authors of this article.

Markus Brändle
Thomas E. Koch
Martin Naedele
ABB Corporate Research
Baden-Dättwil, Switzerland
markus.braendle@ch.abb.com
thomas.koch@ch.abb.com
martin.naedele@ch.abb.com

Rolf Vahldieck
ABB Automation GmbH
Minden, Germany
rolf.vahldieck@de.abb.com

References

[1] **Naedele, M.** Addressing IT Security for Critical Control Systems, 40th Hawaii Int. Conf. on System Sciences (HICSS-40), Hawaii, January 2007.
[2] http://www.sandia.gov/news/resources/releases/2006/logiic-project.html (November 2007)
[3] IDS is dead, Gartner 2003.
[4] **M. Naedele, Biderbost, O.** Human-Assisted Intrusion Detection for Process Control Systems 2nd Int. Conf. on Applied Cryptography and Network Security (ACNS) Tunxi/Huangshan, China, June 2004.
[5] **Koch, T. E., Gelle, E., Ungar, R., Hårsta, J., Tingle, L.** Autonomic computing, *ABB Review* 1/2005, 55–57.

Further reading

Naedele, M., Dzung, D., Vahldieck, R., Oyen, D. Industrial information system security (tutorial in three parts), part 1: *ABB Review* 2/2005, 66–70, part 2: 3/2005, 74–78, part 3: 4/2005, 69–74.