AUTOMATING THE CONFIGURATION OF IT ASSET MANAGEMENT IN INDUSTRIAL AUTOMATION SYSTEMS

Thomas E. Koch, Esther Gelle, Patrick Sager
ABB Switzerland Ltd, Corporate Research
Segelhof, CH-5405 Baden-Dättwi

Keywords: Automated software configuration, IT asset management, network management, automation network, autonomic computing, self-configuration, software architecture

Abstract: The installation and administration of large heterogeneous IT infrastructures, for enterprises as well industrial automation systems, are becoming more and more complex and time consuming. Industrial automation systems present an additional challenge, in that these control and supervise mission critical production sites. Nevertheless, it is common practice to manually install and maintain industrial networks and the process control software running on them, which can be both expensive and error prone. In order to address these challenges, we believe that in the long term such systems must behave autonomously. As preliminary steps to the realization of this vision, automated IT asset management tools and practices will be highlighted in this contribution. We will point out the advantages of combining process control and network management in the domain of industrial automation technology. Furthermore we will give an outlook towards a new component model for Autonomic or Organic Computing for network management and will apply this to industrial automation systems.

1 INTRODUCTION

The installation and administration of large heterogeneous IT infrastructures, for enterprises as well industrial automation systems, are becoming more and more complex and time consuming. The growing number of interconnections between networks, the development of new intelligent IT devices, and increasingly sophisticated computer hardware and software, require in-depth knowledge of IT protocols, interfaces, and standards to manage such infrastructures. The exponential growth of the World-Wide-Web and new IT technologies enable further integration of software and hardware systems across company boundaries. This and the fast technology cycles make it virtually impossible to manage IT infrastructures centrally. And finally, skilled professionals who have the necessary expertise to manage all related topics are increasingly difficult to find. Industrial automation systems, such as those delivered by ABB Inc., present an additional challenge, in that these control and supervise mission critical production sites, which must be up and running 24 hours a day, 7 days a week. Nevertheless, it is common practice to manually install and maintain industrial networks and the process control software running on them, which can be both expensive and error prone. In order to address these challenges, we believe that in the long term such systems must behave autonomously. As preliminary steps to the realization of this vision, automated IT asset management tools and practices are available, this will be described now.

2 PC, NETWORK AND SOFTWARE MONITORING OF INDUSTRIAL AUTOMATION SYSTEMS

ABB Inc. is a leader in power and automation technologies that enable customers to improve performance while lowering environmental impact.

E. Koch T., Gelle E. and Sager P. (2005).
AUTOMATING THE CONFIGURATION OF IT ASSET MANAGEMENT IN INDUSTRIAL AUTOMATION SYSTEMS.
In *Proceedings of the Seventh International Conference on Enterprise Information Systems*, pages 306-311
DOI: 10.5220/0002544003060311

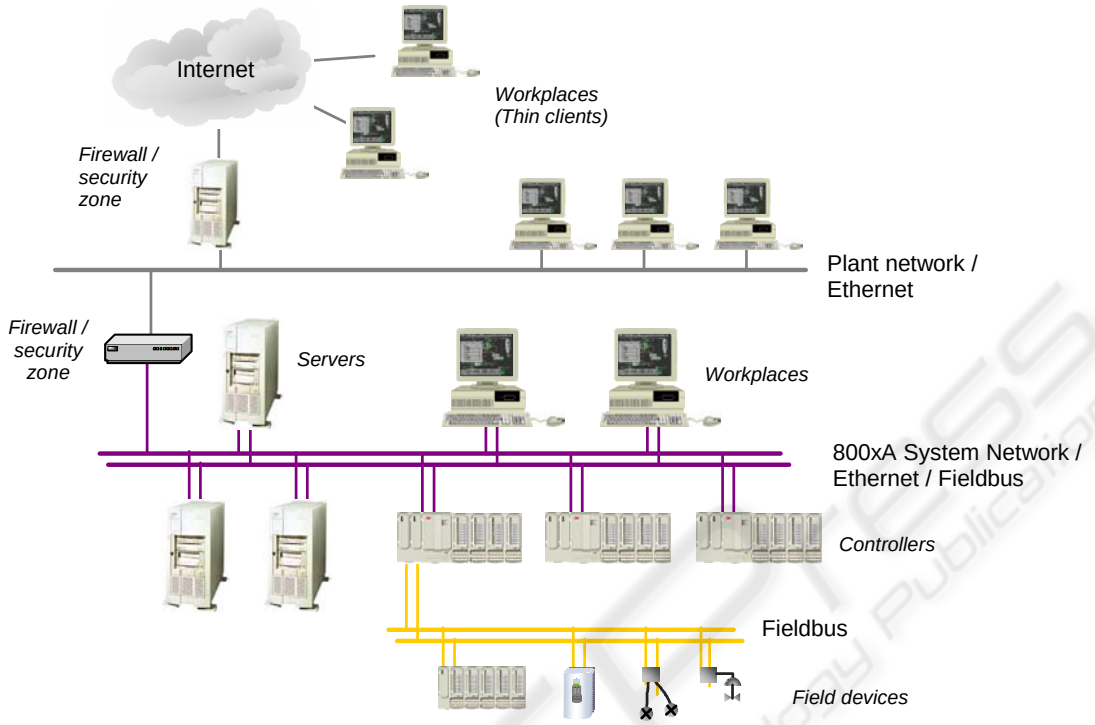

Figure 1: Example of an Industrial Automation Network (with courtesy of ABB Inc.): It consists of many heterogeneous devices like (process) controllers, motors, small machines, routers, switches, servers and client PCs, connected by Ethernet and TCP/IP.

In automation, ABB provides products encompassing several families of process control systems comprising both hardware and software.

Currently ABB provides with its new automation system 800xA an operator platform for typical automation applications that control and supervise for example a cement or steel production plant. A typical industrial automation network consists of several layers: process, field, group control and process control level (Figure 1). The operator workplace is connected to the control network and shows the operator the current status of the process online receiving a continuous stream of data from the controllers using OPC. It is critical for continuous and reliable operation that not only the technical process is supervised but also the control network itself. Even with redundancy built into the control network (Figure 1) a failure of the software running in the controllers or in the operator stations may go unnoticed and thus leave the operator without control over the process (One of the failures provoking the power blackout in August 2003 came from a lack of real-time system monitoring on the part of a system operator and an inability to determine the location or severity of problems, http://www.cbc.ca/news/background/poweroutage/explained.html).

In ABB's 800xA system, the application "PC, Network and Software Monitoring" (PNSM) provides the operator with an overview of the status of the control network and the devices connected to it. It enables the monitoring of IT assets, e.g. computer nodes, routers, printers etc. An IT asset comprises all IT items to be measured such as hard disk usage, network load or number of connections.. The IT item as the basic piece of information is retrieved from Windows Management Instrumentation (WMI) via OPC making use of the fact that 800xA runs on Windows (Policht, 2001). WMI provides an interface for network management applications in Windows and also interfaces to SNMP (Simple Network Management Protocol) (Stallings, 1996). Currently, IT assets are configured manually, based on standard pre-configured asset types, requiring almost no computer expertise. 800xA provides preconfigured asset types from which a specific asset can be instantiated. For example if the hard disk usage of a given computer is to be monitored, the first step is to create an IT Asset Type "Generic Computer Node" which contains as one characteristic the item of interest

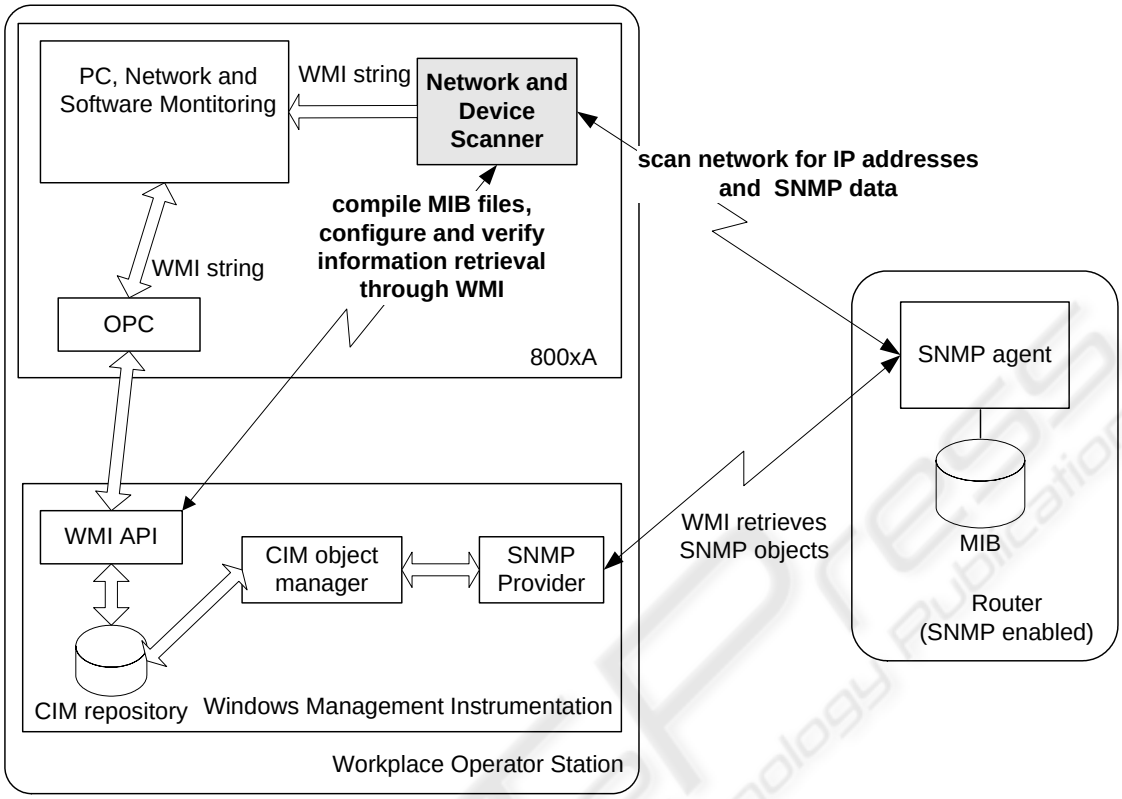

Figure 2: Actual System Architecture: Network and Device Scanner embedded in 800xA and providing support for PNSM.

hard disk usage. From "Generic Computer Node" an instance "Asset 001" is created. The last step consists of configuring "Asset 001" mainly by setting its IP address and the name of the disk drive to monitor. Exactly how information on the hard disk of that specific computer node is retrieved is hidden from the operator. This whole procedure is done with a few mouse clicks.

However, at the initial configuration of the automation system or should new IT asset types need to be created, additional expert knowledge in technologies such as WMI and SNMP is required, as well knowledge of specific data models and formats in which network devices are described, such as Common information model (CIM), Management Information Base (MIB), and Management Object Format (MOF). With the various models and formats go a multitude of tools supporting conversion from one format into another and the loading of a format into the WMI repository. This process is still done manually and thus very error-prone.

3 NETWORK AND DEVICE SCANNING TOOL

3.1 Configuration Process

The main goal of our project was to improve the configuration for later asset monitoring in 800xA and PNSM. If we consider the initial task of setting up a monitoring system for a given control network as shown in Figure 1, we have to scan the network in order identify all IT assets connected to it. Given input will be ranges of IP addresses and SNMP community names. This network scan mainly results in an IP address and some information on the type of asset (computer node, router etc.). If the IT asset type is already known in the 800xA library, a new asset can be created and configured with a few mouse clicks as described in the previous section. If we face an unknown IT asset type, additional data on the asset is to be retrieved in form of IT items (SNMP OIDs) in order to propose a choice on which characteristics should typically be monitored for that IT asset type. Once a decision is taken, the specific characteristics have to be established in form of IT

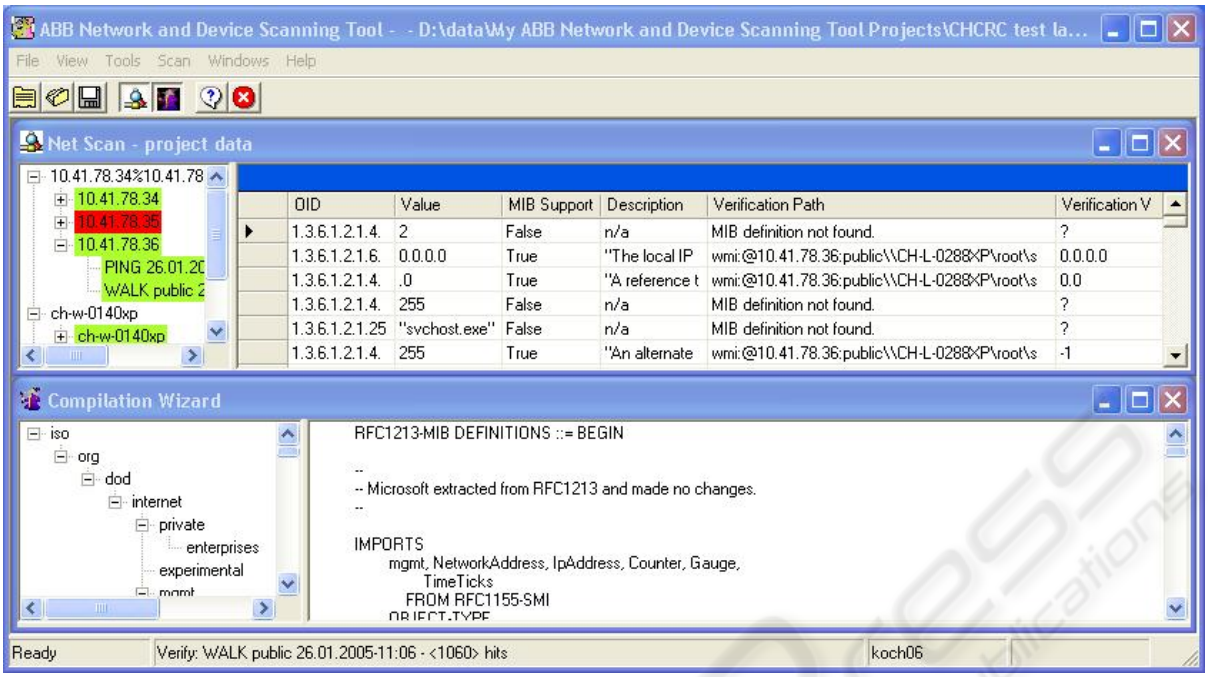

Figure 3: The ABB Network and Device Scanning GUI application consists of two main windows: The NetScan and CompilationWizard forms and shows relevant information to the user.

items as required by WMI, which results in a WMI string. As a verification step the same IT item values are retrieved through SNMP and WMI in parallel and compared. The most engineering-intensive steps in more detail:

1.) Gain an overview of all existing IT assets in a network.
   a) Scan relevant section of the network given by an IP range.
   b) Filter the IT assets or IP hosts that are up
   c) Get descriptions from each IP host using SNMP to discriminate of which type the IT asset is?
2.) Overview of the type of IT items per IT asset.
   a) Use SNMP to retrieve further information on an IT asset in form of SNMP object identifiers (OIDs).
   b) Use existing MIB information loaded in PNSM to get description for each OID (OID mapping).
   c) Allow user to add/remove MIB files to/from the MIB set; redo 2b)
3.) Configuration of IT items as WMI string.
   a) Compile selected MIB files into Windows SMIR (user may remove those as well)
   b) Provide WMI path information to PNSM
4.) Provide a verification step in order to test that an updated MIB is available through WMI. Compare SNMP OID values with WMI counterparts

We assume here that the automation network shown as control network (Figure 1) uses Ethernet and TCP/IP and that all devices have a fixed IP address and an enabled SNMP agent running.

3.2 Implementation

We automated this configuration process with the ABB Network and Device Scanning tool (NDS) as shown in Figure 2. To implement the NDS we followed a component-based SW architecture approach. We defined interfaces and used existing SW components to provide a maximum degree of reusability and independence. Reusable components are for example the MIB parser, the MIB compiler and loader, ICMP echo (ping) and also several SNMP functions. NDS itself consists of classical 3-tier architecture: a standalone GUI application for triggering actions and displaying information, an underlying library containing all application logic and the file system as persistent project data storage. The NDS library is the core comprising the mentioned interchangeable components. It is written in c# utilizing .NET technology.

The GUI -shown in Figure 3- has two main window forms: The NetScan form triggers network scanning activities including ICMP and SNMP protocols, whereas the CompilationWizard form is used to handle MIB activities such as compiling Mibs and loading Mibs into WMI. Let's explain the example of Figure 3 in more detail: The left pane of

NetScan form shows the scanned nodes in a treeview,. By selecting one activity like "Walk public…" the right pane shows more specific information about that node. Each line represents one SNMP OID that has been scanned and maybe successfully verfied through WMI: Thus, if scanned and WMI verified values match, those values may be monitored in 800xA using the given WMI path string. On the other hand, if there is no MIB support, the user has to search for a fitting MIB file and load it into NDS.

The insertion of the configured WMI string into PNSM is currently not automated since in some instances an IT item is not just a raw WMI value (e.g. disk size) but a value calculated from several raw values (e.g. % of disk used = 100* disk space used / disk size). Such user-defined IT items are provided in PNSM through scripts, which use WMI values as a basis.

The search for relevant MIBs that are to be included in PNSM has also not been automated. Currently, the user has to identify new MIBs in an offline process given the type of IT assets.

3.3 Comparison and Discussion

The integration of network management of the automation systems' IT infrastructure into a process control system like ABB's 800xA pays off after a very short time (Seufert 2003). This approach combines process and network supervision into one tool. In our case this integration of network management is achieved by the PNSM OPC server which gets the information from the devices through WMI and delivers directly to the 800xA, as already mentioned. The advantages of this integration are evident:

- One supervision system for the whole automation system instead of two. Network failures are shown in PCS.
- No need for extra IT specialists for network management at run-time. For installation and configuration it is still recommended.

But the installation and configuration of such an integrated approach is very expensive, as stated in former sections. What other tools are available that might support or even automate this error-prone configuration process? How to get the IP and SNMP information into WMI?

There are many tools for IT network management which are often used for security issues as well. Schönwälder gives overviews of different SNMP tools and their architecture (Schönwälder 2001, 2002), Fyodor lists security tools (Fyodor 2004). Additionally there are many commercial network management tools on the market in order to manage enterprise networks. But there is no network management tool that provides all the steps needed to configure and monitor an industrial automation system as described in former sections. Most tools provide net scanning features, some tools are MIB parsers or MIB compilers like Microsofts basic Windows helpers "smi2smir" or "mofcomp". Furthermore, no tool has a verification feature to get the SNMP OID values from the device SNMP agents and through WMI in order to compare them and thus verify the configuration of WMI.

The main benefits of this automation of the former manual configuration steps include reduction time consuming and complex engineering efforts, improvement of the quality of configuration data, and faster integration of new Assets into the Windows operating system repository and PNSM library. Therefore, NDS may result in a significant cost savings for ABB and its customers.

4 OUTLOOK

Currently the tool follows a pull approach in that a user needs to run the network and device scanning functions in order to follow changes in the network. In an approach towards the realization of visions like autonomic or organic computing (Horn, 2001, Kephart et al., 2003, Müller-Schloer, 2004), a new device in the network would automatically register in the ABB Network and Device Scanning tool and activate update mechanisms in PNSM. In a first step, this might include scheduled network scans and analysis of differing information, new devices might be scanned and configured automatically

Concerning the autonomic and organic computing visions, IT networks and its IT assets will be self-aware. These components will have these "self"-characteristics like self- installation and self-configuration, -optimization, -healing and -protection. From our perspective presented in this paper, autonomic IT assets such as computers, routers, switches and controllers, for example ABB's AC800M, could acknowledge, install and configure them selves. Additionally they may inform neighbor components in the network of their existence, e.g. by publishing their offered services.

In order to achieve these goals, the components need to talk the same language. Data structures, protocols and services must be openly standardized and implemented by vendors. Examples in network management include the "Intelligent Platform Management Interface" (IPMI), "Web-Based Enterprise Management" (WBEM) of the Distributed Management Task Force organization

(DMTF), "Structured Management Information" (SMI) definition and the "Simple Network Management Protocol" (SNMP) of the Internet Engineering Task Force (IETF) community. (DMTF and IETF are in charge to standardize the architecture and integration technology for enterprise and Internet environments.)

5 CONCLUSION

In this paper we discussed the complex problems of configuration and execution of network management of industrial automation systems, especially for monitoring purposes. We showed how ABB solves this nowadays with its process control system 800xA (including PNMS and NDS tools). The Network and Device Scanning tool provides a new way to configure Microsoft Windows WMI for later monitoring of the network. It gathers IP and SNMP data from the automation network and other sources like MIB files, maps the different data and compiles them into SMIR/WMI. The main benefits of this automation versus the former manual configuration steps include reduction time consuming and complex engineering efforts, improvement of the quality of configuration data, and faster integration of new Assets into the Windows operating system repository and PNSM library. Thus, for ABB and its customers, NDS may result in the following benefits: Improved productivity of engineering personnel installing and configuring IT assets, improved reliability through online monitoring of the IT assets and improved quality of real-time monitoring information for service and support personnel.

We pointed out the advantages of combining process control and network management in the domain of industrial automation technology. Further activities include issues concerning network load and analysis.

REFERENCES

DMTF, *Distributed Management Task Force*, Retrieved October 26, 2004, from http://www.dmtf.org/

Fyodor, 2004, Retrieved October 22, from http://www.insecure.org/

Horn, P., 2001. *Autonomic Computing: IBM's Perspective on the state of Information Technology.*

IETF, *The Internet Engineering Task Force*, Retrieved October 26, 2004, from http://www.ietf.org/

Industrial IT System 800xA, System Architecture. 3BUS092080R0001. *ABB Automation Technologies*. Retrieved October 18, 2004, from http://www.abb.com - Products & Services – ABB Product Guide – 800xA.

IPMI, *Intelligent Platform Management Interface*, Intel, Retrieved October 26, 2004, from http://www.intel.com/design/servers/ipmi/

Kephart, J. O., Chess, D.M., 2003. The Vision of Autonomic Computing. *IEEE Computer*. 41-50.

McKinley, P.K., Sadjadi, S.M., Kasten, E.P., Cheng, B.H.C., 2004, Composing Adaptive Software. *IEEE Computer*. 56-64.

Müller-Schloer, C., von der Malsburg, C., Würtz, R.P. August 2004, *Organic Computing*. Informatik Spektrum, 332-336.

OPC. *OPC Foundation*. Retrieved October 22, 2004, from http://www.opcfoundation.org.

Policht, M., 2001. *WMI Essentials for Automating Windows Management*. Sams.

Preiss, O., Naedele, M., 2002. Architectural Support for Reuse: A Case Study in Industrial Automation. In *Building Reliable Component-Based Software Systems*. Eds: Crnkovic, I., Larsson, M., Artech House Publishers.

Schönwälder, J, 2001, *Specific SNM Tools*, 15th Usenix Systems Administration Conference (LISA 2001), San Diego

Schönwälder, J, 2002, *Evolution of Open Source SNMP Tools*. 3rd System Administration and Networking Conference (SANE 2002), Maastricht

Seufert, F., 2003. Netzmangement der Zukunft, *megalink*, 27-29 (In German).

Stallings, W., 1996, *SNMP, SNMPv2,and RMON – Practical Network Management.* Addison-Wesley. 2nd edition.

WBEM, *Web-Based Enterprise Management Initiative*, Retrieved October 26, 2004, from http://www.dmtf.org/standards/wbem