CARNEGIE MELLON UNIVERSITY
INFORMATION NETWORKING INSTITUTE

SECURING CRITICAL UTILITY SYSTEMS & NETWORK INFRASTRUCTURES

Bruno Miguel Inácio Garrancho

Thesis Committee:
Paulo Jorge Esteves Veríssimo, Advisor
António Casimiro Ferreira da Costa, Reader
Hans Peter Reiser

Submitted in partial fulfillment of the requirements for the degree of
MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY - INFORMATION SECURITY

November 2009

UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

SECURING CRITICAL UTILITY SYSTEMS & NETWORK INFRASTRUCTURES

Bruno Miguel Inácio Garrancho

MESTRADO EM SEGURANÇA INFORMÁTICA

November 2009

UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

SECURING CRITICAL UTILITY SYSTEMS & NETWORK INFRASTRUCTURES

Bruno Miguel Inácio Garrancho

Orientador
Prof. Doutor Paulo Jorge Esteves Veríssimo

MESTRADO EM SEGURANÇA INFORMÁTICA

November 2009

Resumo

As infra-estruturas críticas de TI para serviços públicos são apoiadas por inúmeros sistemas complexos. Estes sistemas permitem a gestão e recolha de informação em tempo-real, constituindo a base para a gestão eficiente das operações. A utilização, cada vez mais frequente, de software e hardware (Commercial Off-The-Shelf, COTS) em sistemas SCADA permitiu grandes beneficios financeiros na aquisição e desenvolvimento de soluções técnicas que suportam os serviços públicos. O uso de hardware e software COTS em sistemas SCADA transferiu para as infra-estruturas críticas os problemas de segurança de uma infra-estrutura de TI empresarial.

Neste contexto, um desafio para as equipas de gestão operacional dos sistemas de TI é a gestão eficaz dos sistemas e redes que compõem as infra-estruturas críticas dos serviços públicos. Apesar de estas organizações adoptarem, cada vez mais, normas e melhores práticas que visam melhorar a gestão, operações e processos de configuração.

Este projecto de investigação propõe-se a desenvolver um estudo comparativo de plataformas de gestão integrada no contexto dos sistemas SCADA que suportam serviços públicos. Adicionalmente, este projecto de investigação irá desenvolver estudos acerca de perfis operacionais dos Sistemas Operativos que suportam a infra-estrutura IT dos serviços públicos críticos. Este projecto de investigação irá descrever como as decisões estratégicas de gestão têm impacto nas operações de gestão de uma infra-estrutura TI.

Palavras-chave: SCADA; Segurança; Monitorização; Sistemas Operativos; Plataformas de Gestão Integrada;

Abstract

Modern critical utility IT infrastructures are supported by numerous complex systems. These systems allow real-time management and information collection, which is the basis of efficient service management operations. The usage of commercial off-the-shelf (COTS) hardware and software in SCADA systems allowed for major financial advantages in purchasing and developing technical solutions. On the other hand, this COTS hardware and software generalized usage in SCADA systems, exposed critical infrastructures to the security problems of a corporate IT infrastructure.

A significant challenge for IT teams is managing critical utility IT infrastructures even upon adopting security best practices that help management, operations and configuration of the systems and network components that comprise those infrastructures.

This research project proposes to survey integrated management software that can address the specific security constraints of a SCADA infrastructure supported by COTS software. Additionally, this research project proposes to investigate techniques that will allow the creation of operational profiles of Operating Systems supporting critical utility IT infrastructures.

This research project will describe how the strategic management decisions impact tactical operations management of an IT environment. We will investigate desirable technical management elements in support of the operational management.

Keywords: SCADA; Security; Monitoring; Operating Systems; Integrated Management Platforms;

Acknowledgments

I would like to thank Carnegie Mellon University, Information Networking Institute, and Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, for their dedication to this project.

I would like to thank Professor Paulo Veríssimo for his guidance during the development of this research project.

I would like to thank Luís Barruncho and Logica for believing in me and supporting my work during the last year.

I would like to thank Paulo Moniz and Miguel Areias for their insigth during the development of this project.

I would like to thank my colleagues Benjamim Durães, Carlos Silva, Elisa Páscoa, Eugénio Pinto, João Borralho, João Ramos, Luís Sousa, Nuno Loureiro, Ricardo Ramalho, Sérgio Nunes and Tiago Mendo. You have been great journey companions and I have learned from all of you.

I would like to thank Patrícia and my parents for their patience during the course of this endeavour.

"Dream in a pragmatic way.", Aldous Huxley

Lisboa, November 2009

Dedicated to Patrícia

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Modern Critical Utility IT Infrastructures are supported by numerous complex systems. These systems allow real-time management and information collection, which is the basis of efficient service management operations. SCADA stands for Supervisory Control And Data Acquisition and it serves to designate these types of systems.[1]. The main function of SCADA systems is to provide accurate, and as close to real-time, information while allowing operators to respond to events in order to maintain the functional requirements of a system.

To support the communication of SCADA data a communication network must be in place. Traditionally these communication systems operated proprietary protocols on fixed telephone landlines and modems. As communication networks evolved, TCP/IP based technology became an efficient way of communicating SCADA data. TCP/IP was used to overcome some of the legacy problems and also allowed for more flexibility in terms of scalability and operations.

As with communications, systems and hardware also became more mainstream and with that, the usage of COTS (commercial, off-the-shelf) hardware and software in SCADA systems allowed for major financial advantages in purchasing and developing. On the other hand, this COTS hardware and software generalized usage in SCADA systems, exposed critical infrastructures to the security problems of a corporate network.

A significant challenge for IT teams managing Critical Utility IT Infrastructures are management, operations and configuration of the systems and network components that comprise those infrastructures. The management knowledge travels from the corporate world

into a distinct paradigm. Usually, the properties that have to be achieved by the systems supporting critical infrastructures differ from those on the corporate world.

One source of security concerns is the operational management of the IT infrastructure. Operations can drive a system, and potentially the whole IT infrastructure, to an insecure state. As the systems that support the SCADA operations rely more on COTS hardware and software, infrastructure security relies on extending operational procedures common on corporate infrastructures to the SCADA infrastructure domain. Another important aspect of these SCADA infrastructures is that they are in constant evolution in response to the company's demands. This puts an even greater stress on the operational management staff capabilities, and often security problems originate in erroneous operational configurations.

One extremely important threat to critical utilities is Cyber-Terrorism which, in general terms, relates information technology to unconventional warfare attacks. In [2], Purpura draws a broad picture of the practical implications of Terrorism for the United States of America, but his reasoning is quite accurate for other country's reality. In his characterization of terrorism he describes specific forms of terrorism, like Cyber-Terrorism. Common sense and history have proved, numerous times, that utilities are a natural target in conventional warfare and unconventional warfare scenarios.

By 2005, the SmartGrids European Technology Platform for Electricity Networks of the Future started with the promotion of a new vision for the development of European electricity networks[3]. For this vision to become reality it is required that all the stakeholders, involved in the project, are aware of the challenges that lay ahead. Some of these foreseeable challenges are heavily dependent on information and communication technologies and the resilience of those technologies to failures or attacks.

This research project will focus on establishing the grounds to achieve a dependable operational environment for a critical utility IT infrastructure. We will establish a strategy to maintain a dependable environment, based on COTS software, and survey operational management platforms, from several industry vendors, accessing their coverage for the tactical requirements of such an environment.

One of the goals of this project is to investigate techniques that will allow the monitorig of COTS systems supporting criticl utility IT infrastructure. This information has significant value for day-to-day operations and can also be used in behavior-based intrusion detection, note that behavior-based detection can coexist with signature-based detection in such infrastructures. System monitoring is a starting point for a complete security management process which includes assessing risks and threats, product vulnerabilities and new attack vectors. This work will enable the operational management team to create strategies and

plans for detection of threats and protection of the SCADA IT infrastructure.

1.2 Contributions

This research project is a subset of an ongoing major effort to improve the security of the SCADA system for a European Electric Power Company.

The starting point for this research project is the necessity to evaluate tools that will enable a global strategy of Defense-in-Depth of the complete critical utility IT infrastructure. One important goal is detailing a plan for the evolution of a reliable management platform on which next generation demands can be met without compromising security.

This research project will include studying several techniques of monitoring of OS information. The gathered information will promote the creation of a plan to supervise the SCADA IT infrastructure. A first step will require the study of IT operations management platforms, these platforms will allow the collection of relevant metrics and events on which the operational management of the SCADA IT infrastructure can define security policies. The collected information will in turn be correlated with other information (NIDS, firewall logs) to achieve full coverage of the IT infrastructure.

Furthermore, this research project will focus on studying the Microsoft Windows Operating System architecture supporting these critical information systems in order to investigate systems analysis techniques which can help identify threats to systems and, ultimately, the whole infrastructure.

Chapter 2

Critical Utility IT Infrastructures Security Management

2.1 IT Infrastructure Service Management

The growing complexity and evolution of IT infrastructures lead to IT Service Management concept. Winniford et.al., studied the currently adopted concepts and frameworks [4]. The study concluded that the broad definitions of the concepts and frameworks are sufficient for the upper management requirements of the IT Service Management process. The frameworks studied aim at managing service of generic IT infrastructures and are extremely valuable in order to relate the Critical Utility IT Infrastructure to the upper management business requirements. One interesting concept of IT Service Management is the ”functional silos” concept, i.e. aggregation of IT services with end-to-end definitions for availability and performance, that concept loosely relates to the defense-in-depth strategy for achieving dependable Critical Utility IT infrastructures.

IT Service Management concepts have grown out, among others, of the Information Technology Infrastructure Library - ITIL[5]. Currently the IT community discusses the exact scope and overlapping of IT concepts, such as ITSM, ITIL, Control Objectives for Information and related Technology - CobiT[6]. Additionally, the International Standards Organization (ISO) ratified ISO/IEC 20000 a standard that brings together these several paradigms under a common set of principles, which can be generally defined as IT Service Management.

Next, we characterize some of these views on IT systems management. This description serves to situate Critical Utility IT infrastructures management in the complex management

scenario of an organization.

2.1.1 ITIL

General recognition of IT service management needs resulted in the definition and rise of ITIL, a set of books describing best practices in several areas of service management. Currently the scope has been broadened to include a life-cycle perspective on service strategy, design, transition, operation, and continuous improvement. ITIL service support consists of several sub-processes for making structured changes to the infrastructure. ITIL service delivery defines sub-processes for maintaining the infrastructure running at agreed-upon levels, including Service Level Management - SLM as one of those sub-processes.

2.1.2 IT Governance

Started by the audit abuses that prompted the Sarbanes-Oxley Legislation - SOX [7], IT governance is yet another term subject to broad and narrow definitions. IT Governance in a strict sense is the appropriation of decision rights in an organization structure, and in a broad sense is the overall strategy. This strategy definition includes risk, financial, and process management. IT governance does not address the daily management of an IT organization.

2.1.3 CobiT

The Information Systems Audit and Control Association - ISACA [6] has developed the Control Objectives for Information and related Technology to translate another paradigm of IT management concepts. CobiT groups IT governance objectives into areas covering: Planning and organizing; Acquiring and implementing; Delivering and supporting; Monitoring and evaluating. The CobiT framework seeks to create business controls and accountability while still viewing IT service in terms of functional silos .

2.1.4 ITSM

In 2005, the International Standards Organization - ISO ratified ISO/IEC 20000 [8] which, again, brings together several service management streams under a common set of principles, which are generally called IT Service Management. It defines both a specification

and a code of practice for service management. The service delivery areas of IT operations management have little, to none, published academic research. Researchers are still trying to determine the industry maturity, understanding and adoption of IT Service Management practices.

2.2 IT Infrastructures Security Management Process

Security management planning requires the creation, deployment, and enforcement of a security policy. The most effective way to address security management planning is using a top-down approach. The definition of security policies for the organization is, the responsibility of the upper management, usually based on the concepts described in Section 2.1. These security policies provide direction to the lower levels of the organization's hierarchy. The responsibility of middle management is to, starting from the security policy, adopt and develop standards, baselines, guidelines, and procedures. The operational managers must then deploy the configurations detailed by the security management documentation and monitor the system for exceptions to the security policy.

In a broad sense a key function of most organizations is to "maintain security". Every organization is interested in securing its assets, its information and its business. The process of designing, implementing and operating IT infrastructures is complex and, therefore, risk prone. To better manage IT infrastructure security design, implementation and operation those processes have been, to some extent, formalized. A goal of the process formalization is to transform the complexity of the IT security design, implementation and operations into a manageable process which allows for accountability and verification.

The formalization of security process can be viewed as an hierarchical organization of information and documentation. The top level of this formalization can be viewed as a security policy, i.e., a definition of the scope of security mechanisms needed by the organization in relation to assets that need protection. The following layer can be viewed as security standards, baselines, and guidelines which is a more detailed technical guidance for the enforcement of the security policies. The bottom layer is comprised of security procedures, i.e., a detailed technical description of a specific security mechanism, control, or solution.

Most of the reasoning in this section is a direct match to corporate world current panorama, but also a valuable starting point when addressing Critical Utility IT Infrastructures.

2.3 IT Infrastructures Security Management Concepts

Security management concepts and principles are fundamental elements of a security policy. They define the parameters needed for a secure environment. They also serve as goals and objectives that both policy creators and implementers must achieve in order to create a secure environment.

The primary goals and objectives of security are as follows:

- Confidentiality
- Integrity
- Availability

We shall not go into extensive description given that these security principles have been subject to much discussion and tend to be common sense for the security field practitioners.

Security controls are usually evaluated on whether they address these core information security principles. Vulnerabilities and risks are also evaluated based on the threat they pose against one or more of the goals and objectives stated above.

In corporate environment each of the principles tends to have the same relative weight in relation to the other two in every stage of the security management planning process. This research project will focus on the operational aspects of Critical Utility IT infrastructures in regards to achieving, what are understood as the primary goals and objectives of security.

Also, when designing a security policy and deploying a security solution there are also other security principles that need to be addressed, namely: privacy, identification, authentication, authorization, accountability, non-repudiation and auditing.

Along with the security concepts, this research project also considers protection mechanisms. They represent some of the characteristics of security controls, namely: layering, abstraction, data hiding and encryption. The security controls offer their protection for confidentiality, integrity, and availability through the use of these mechanisms.

One important aspect of security management is the management of change. Change in a secure environment can lead to vulnerabilities. To maintain security in the face of change requires to systematically manage change. To achieve this systematic approach requires extensive planning, testing, logging, auditing, and monitoring of activities related to security controls. The records of changes to an environment can be used to identify agents of change, whether those agents are objects, subjects, programs, communication pathways, or

even the network itself. A goal of change management is to ensure that any change does not lead to reduced or compromised security situation.

2.4 Operational Management of Critical Utility IT Infrastructures

Most companies are aware that day-to-day operations of their corporate IT infrastructure can be a source of security related problems. IT best practices are usually aligned with business requirements,i.e. IT Service Management. One of the basic goals of an IT organization is to optimize server and application availability and performance.

Continuous optimization of the Critical Utility IT Infrastructure is a fundamental role of the Operations Management team. One significant challenge these IT teams face is achieving the balance between efficient and cost effective management. This is due, mainly, to two factors: the *functional silos*, teams specialized in a specific IT technology; and the tools or management platforms are unique, within the *functional silos*, in support of operations. Difficult cooperation between distinct *functional silos*, due to proprietary interfaces, has an impact on the efficiency of the management environment. Not forgetting that new applications introduced in support of business requirements require, themselves, specialized management and monitoring. Given the above scenario, it is clear that root cause analysis of incidents impacting business can be an challenging task in such a scenario. We can also state that, to some extent, the existence of independent *functional silos* prevents the adoption of management processes, like the ones described in Section 2.2.

Those management process controls, described in Section 2.2, are becoming a mandated requirement for most corporations and critical utilities companies are no exception. This shows the inter-relations between corporate management processes and IT operations management. Additionally, all this reasoning justifies the importance of cross-*functional silos* integrated management.

Chapter 3 describes into technical extent the requirements of integrated management platforms.

2.5 Defense in Depth and Information Assurance in Critical Utility IT Infrastructures

One easy parallel to trace while addressing Critical Utility IT infrastructures is that of information in support of military operations [9]. The management of SCADA systems requires timely and accurate information, just like military warfare operation. Defense in Depth strategy relates to managing in an integrated manner the capabilities of teams, operations and technology to achieve effective, multi-layer, multi-dimensional resilience to possible attacks on the infrastructure. The goal is to delay the advance of the attacker by maintaining multiple, layered lines of defense rather than one strong defensive line, perimeter defense.

In terms of infrastructure security, defense in depth is a security strategy wherein defenses are overlapped so that a breach in one layer only leads the opponent to the next layer of defenses. Layering defenses helps to prevent direct attacks against critical systems and data, increases the probability of the attack being detected, and provides the defender with more time to reconfigure defenses to where they are really needed in the event of an attack. In figure 2.1 we provide a vision of defense in depth with relation to a critical utility infrastructure.

The layers of defensive positions in defense in depth can be described as follows:

- Data. An attacker's first choice target. Databases, service information, documents contain deep knowledge on the operational scenario and tend to be trampolines to more broad attacks.
- Application. The software that manipulates the data that is the ultimate target of attack.
- Host. The systems that are running business critical applications.
- Internal Network. The network infrastructure.
- Perimeter. The network that connects the IT infrastructure to other networks, such as to external users or application support.
- Physical. The tangible aspects in computing. Computers, network devices, facilities.
- Security Management Process. The overall governing principles of the security strategy.

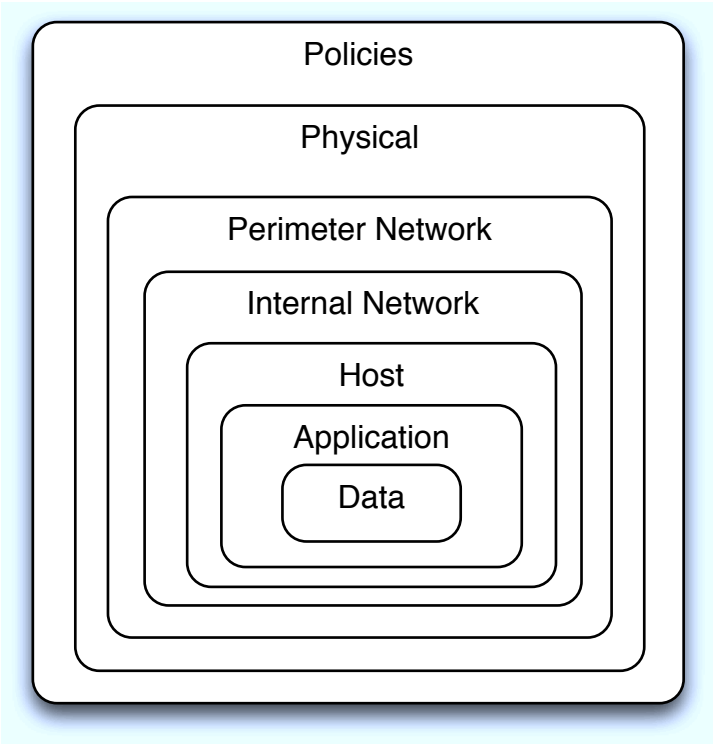

Figure 2.1: Defense in Depth Layers

Host and *Application* are the main concerns of our research project. The details investigated in this research project are strictly linked to those areas of security. This approach eases the separation of duties and concerns among distinct *functional silos* of an organization, and thus eases the roll-out of this project onto an organization adhering to this strategy.

An important principle that guides defense in depth is achieving Information Assurance. Information Assurance is an holistic principle that relates protection coverage from attacks, by application of security mechanisms, to assure confidentiality, availability, integrity, authentication and non-repudiation. It is clear to say that achieving Information Assurance requires an organic relationship between three key elements: people, technology and operations.

People

Senior level management commitment, based on a clear understanding of the perceived threats, is a key point in the whole strategy of defense in depth. This must be followed with effective policies and procedures, clear definition and assignment of roles, training of users and system operators, and infrastructure wide personal accountability and audit-ability. This includes the establishment of physical security and personnel security measures, the

goal is to control and monitor access to facilities and elements of the IT infrastructure environment.

Technology

Currently, a wide variety of technologies are available in support of Information Assurance. To insure that the right technologies are procured and deployed, any organization should establish a strict policy for technology acquisition. Where and how to deploy these technologies should be defined along the lines of Defense in Depth strategy.

In critical utility IT infrastructures the focus should be on the following general areas:

Networks - An organization needs to deploy security mechanisms at multiple locations to handle all classes of attacks. Adversaries can attack a target from multiple points using either insiders or outsiders. These defensive standpoints should include defending the networks and communications infrastructure. The protection mechanisms should include providing confidentiality and integrity protection for data transmitted over these networks, protection from Denial of Service attacks should also be included in both the local and wide area communications networks.

Boundaries - Firewalls and intrusion detection systems to address active network attacks. Defend the computing environment by providing adequate access controls on hosts to resist insider attacks.

Layering - Even the best available products have inherent weaknesses and finding an exploitable vulnerability in a system is just a matter of time and effort. To address this problem organizations must deploy multiple defense mechanisms between the attacker and his target. Each of these mechanisms must present unique obstacles to the adversary and optimally should include both protection and detection measures. These measures help increase risk of detection for the attacker while reducing his chances of success or making successful penetrations unaffordable.

Robustness - It is necessary to specify the security strength of protection components as a function of the value of what's it is protecting and the threat at the point of application, risk management. Additionally choosing where to deploy stronger mechanisms is also of significant importance to the overall strategy.

Detection - Mechanisms should be in place in the managed infrastructures to detect intrusions, analyze and correlate the results and react accordingly. The goal is to turn

infrastructures into helpers of the Operations staff. These mechanisms should allow Operations staff to identify if the infrastructure is being attacked, what are sources and targets of the attack and what further measures are needed to correct the situation.

Operations

Operations focuses on all the activities required to maintain an organization's security posture on a day to day basis. These activities include:

- Managing the security evolution of the deployed technology (e.g. installing patches, managing access control lists) ;
- Providing secure key management services ;
- Performing system security assessments to assess the readiness status of the infrastructure ;
- Monitoring and reacting to current threats ;
- Attack sensing, warning, and response ;
- Recovery and reconstitution ;

In Chapter 4 we further analyze technical details of defense in depth in a critical utility IT infrastructure

2.6 CRUTIAL - CRitical UTility InfrastructurAL resilience

CRUTIAL is a project of the Information Society Technologies program of the European Commission[10]. Part of what is proposed by the authors is a blueprint for a distributed systems architecture that serves as a reference for modern critical information infrastructures. The authors propose a set of classes of techniques and algorithms based on paradigms providing resilience to faults and attacks in an automatic way.

CRUTIAL's vision resides in modelling interdependent infrastructures and taking into account the multiple dimensions of inter-dependencies. Additionally providing new architectural patterns, resilient to both accidental failures and malicious attacks. There are several

goals of interest, in the scope of this research project, namely: investigation of models and architectures that address scenarios of openness, heterogeneity and evolution that electrical utilities infrastructures are being subject to; analysis of faults in the information infrastructure that can cause significant impacts on the controlled electric power infrastructure; investigation of distributed architectures enabling dependable control and management of the critical utility IT infrastructures.

As part of the the project, Verissimo, P. and Ferreira Neves, N. and Correia, M. propose a blueprint for a reference critical information infrastructure architecture[11].

The proposed solution encompasses a range of mechanisms of incremental effectiveness, to address from the lowest to the highest importance operations in a critical utility IT infrastructure. They propose architectural configurations with trusted components in key places to induce prevention of some classes of attacks. Together with middleware based automatic tolerance of the remaining faults and intrusions.

This is a comprehensive and extensive project that introduces several new paradigms to the management of critical utilities infrastructures and will certainly change the way critical utility IT infrastructures are designed and planned in the foreseeable future.

2.7 Management Standards & Critical Utility IT infrastructures

SNMP was proposed for the unification of the management information and of the administration protocols, over IP based networks [12]. SNMP is an application-layer protocol which can serve as a platform for the monitoring and management of network attached devices. It is commonly used in the corporate world as a unified mechanism to monitor the status and operation of a diverse range of equipment.

The architectural model of SNMP, master-slave, permits the management and monitoring of network attached devices by the direct polling and query of an SNMP agent by a master, or the receipt of monitoring notification, a SNMP trap, by a master from a slave. The operational elements that are exposed to monitoring or management through the SNMP protocol are typically referred to as objects. A list of these objects is referred to as a management information base (MIB). These MIBs are highly variable and while there are some recommendations there is no fixed set of mandatory rules. At a conceptual level the structure of the SNMP protocol makes it adequate for monitoring critical utility IT infrastructures.

WS-Management [13] is another standard that addresses IT management by providing a common platform for systems to exchange management information across the IT infrastructure. In its core are Web Services and XML flexibility tied together to manage IT infrastructures. While it enables more management capabilities than SNMP, its overhead may compromise attempts to use it in a critical utility IT infrastructure scenario.

2.8 Security Challenges in Critical Utility IT infrastructures

Modern critical utility IT infrastructures are commonly TCP/IP based environments, much as the corporate infrastructure for managing the business that drives operations in a control system, there are technology related vulnerabilities that need to be addressed. Clearly, the main concern as control systems become part of these large architectures is providing security procedures that cover the control system domain as well.

Network-based communications have security issues that must be addressed in the control system domain, since vendor-specific protocols and assumed legacy system security is not always adequate to protect these critical utility IT infrastructures. Examples of threats in open systems architectures that can migrate to control system domains include: hostile code, escalations of privileges, network reconnaissance and data gathering, covert traffic analysis. With successful intrusion into control systems networks come new issues like: attacks on operator consoles, unauthorized access into high security critical networks and remote facilities.

There are key differences between traditional IT architectures and critical utility IT infrastructures systems technology that impact the way to address security problems. From a mitigation viewpoint, deploying IT security technologies into a critical utility IT infrastructure may not be a viable solution. Even if critical utility IT infrastructure use the same protocols that are used in corporate networks, the very nature of control system functionality may turn otherwise appropriate security technologies inappropriate. These systems have usually high time sensitive requirements, so latency and throughput associated with security mechanisms may introduce unmanageable delays and produce high impact on overall system performance. Table 2.1 highlights common security elements present in a corporate infrastructure opposed to critical utility IT infrastructure.

One way to address these differences and their impact is to move into a defense in depth strategy, as described in Section 2.5. Additionally, the importance of an integrated manage-

Security Topic	Corporate IT	Critical Utility IT Infrastructure
Anti-Virus	Common	Uncommon
Technology Lifetime	3-5 years	Around 20 years
Patch Management	Usual	Rare
Change Management	Easy to maintain	Highly complex
Timeliness Constraints	Unspecified delays are accepted	Delays are unacceptable
Availability	Service interruption subject to SLA	Continuous
Facilities	Concentrated in few locations (mostly)	Geographically disperse

Table 2.1: Corporate VS Control Systems

ment systems and platforms has been subject to much discussion in the field of distributes systems, Veríssimo P. et al. [14]. These platforms concentrate several functions that are normally performed by isolated tools and allow infrastructure wide management. Naturally, some of the differences of the two worlds, corporate versus critical utility IT infrastructure, cause impairments that prevent adoption of a more dynamic management approach. The adoption of infrastructure wide platforms is a complicated subject to address and efficiently study outside real testbed scenarios.

In Chapter 3 we investigate the coverage and depth of some of these system management platforms and validate if they are adequate to produce a positive impact in regards to overall security of a critical utility IT infrastructure and its control systems.

Chapter 3

Survey of IT Systems Management Software

IT systems management is a broad area which includes many related products and platforms. There is a multitude of vendors that provide the widest technological coverage.

The importance of IT systems management is increasing, as enterprises mature in terms of their attitudes to IT infrastructures and demand greater visibility into IT operations. IT systems management solutions also have an important role in measuring the return on IT investments. The automation of IT is another emerging function of IT systems management that has become an important priority for enterprises seeking to improve their efficiency, and enhance the alignment between their IT priorities and their business priorities. IT systems management allows enterprises to rationalize their IT spend, while simultaneously improving the efficiency of business operations and enabling self-maintaining and self-managing IT systems. Critical utility IT infrastructures are part of this evolution.

3.1 Trends and Evolution

IT systems management solutions are evolving rapidly due to their broad scope and the fact that they are embedded in many business and technology processes within the enterprise. This section discusses important trends affecting the IT systems management platforms.

Rising energy prices and an increased awareness of climate change have resulted in a much greater focus on reducing energy consumption in the enterprise with a focus on data centers and IT asset management. IT systems management solutions are key components in

implementing power saving strategies and is expected that IT systems management offerings will bring together IT and facilities management under one view. This trend will also lead to greater integration between IT management and facilities management, since power management requirements span both functional areas.

Enterprises are facing challenges in grasping the full benefits of their virtualization deployments. This is due to the difficulty in managing numerous virtualized servers, adequately defining granular roles for servers, availability and performance. IT service management platforms are expected to provide the appropriate technologies to address this challenge and enable virtualization benefits. Virtualization management is also an crucial element of green IT since it allows more efficient utilization of server hardware, along with an expected reduction in the number of physical servers.

The rapid adoption of new communication technologies such as next generation networks and enterprise voice-over-Internet protocol - VoIP - is changing telecommunication networks and enterprise networks. IT applications and standard IP technologies have now replaced proprietary network applications and this fact is removing the distinction between telecommunications networks and IT networks. The cost savings relating to a single network are linked with additional risk and complexity, since that all communications will take place in this new paradigm. With all application data, user data, voice all routed through one network, it is of critical importance that this network is managed in a reliable and effective manner.

Application management in IT systems management platforms has been focused on application availability and reliability. Naturally as the importance of applications, in an enterprise, increases so does the role of application performance management. The need for measuring the quality and performance of application services is driven by the move towards service oriented architecture - SOA - and the increasing prevalence of software-as-a-service - SaaS - business models. Measuring an application's availability along with its performance and speed will support important metrics on the IT infrastructure. This is specially important for managing time-sensitive applications in a critical utility IT infrastructure.

The importance of information and the risk associated with managing it are gaining visibility from the enterprise community. Enterprises need to be aware of their IT assets, specially sensitive information, the increasing regulatory pressure from authorities requires enterprises to monitor access to their data and systems activity, and audit it. This need forces IT systems management platforms to increase its level of integration with security information. Along with delivering reliable tools to monitor IT systems for auditing,

IT governance, and security purposes, IT systems management platforms should handle any issues that affect global system stability. Auditing and monitoring are also extremely important in managing, streamlining system change and configuration.

Service management, which is an integral part of an effective IT systems management strategy, is a key component of IT and business alignment because it provides the ability to measure the value of IT systems to the business.

3.2 IT Systems Management Platforms

In the course of the research project we evaluated several IT systems management platforms in order to provide a central point of IT operations information and also a platform to deliver and aggregate security related information.

Our focus was evaluating the capability to extract system and application information, and thus enable proactive prevent reliability and availability issues. The targeted systems are all Windows OS hosts, with few exceptions, so we considered the specific details of a Windows system in the survey process. Although the reach of these management platforms can be superimposed, by network monitoring solutions and configuration management solutions, the infrastructure environment remains quite static and currently lacks broad and deep operational insight.

Before we continue let us make a brief note on how the operations management software performs its job and the impact it can possibly have on a critical utility IT infrastructure. These platforms manage systems that can be agent-managed computers or agent-less managed computers. A critical utility IT infrastructure has two major distinct scenarios of operation for COTS software namely, central servers and control systems hosts. So to some extent the problem of managing a critical utility IT infrastructure is similar to that of desktop and server management of the corporate IT world.

3.3 Survey of Vendors and Platforms

This information was surveyed from May to November 2009.

Throughout the years HP and IBM have been very innovative in terms of technology and have coupled their technology know-how with planned evolution and customer focus. They both, IBM and HP, have very advanced technical features, IT concepts and significant market experience.

CA has invested in technology and has differentiating capabilities of IT and data center automation, and this is a key point in the IT systems management market.

Microsoft has made significant advances in its IT systems management technology. With the release of its System Center 2007 solution, Microsoft has broadened and improved its IT systems management offering in terms of quality and coverage. It has also enhanced its support for other platforms, thereby removing a key barrier against the adoption of its IT systems management product offering. Microsoft's technology still lacks the maturity and breadth of more established products.

BMC's has a broad portfolio and very strong support for Business Service Management and mainframe management.

While the open source community creates and maintains several alternatives to the commercial systems they are simply monitoring solutions that store collected events by the agents. Of the surveyed solutions only the commercial products performed root cause analysis and service dependency hierarchy mapping.

3.3.1 BMC

BMC offers a portfolio of Business Service Management (BSM) solutions that aim at providing a unified platform for managing IT infrastructures[15]. BMC offers solutions across an entire IT organization but its main focus is consulting services. Next, follows a description of the management platforms and tools, per functional area, offered by BMC that are designed to addresses the problems of managing a critical utility IT infrastructure.

BMC Atrium CMDB & **BMC Atrium CMDB Enterprise Manager** is comprised of a data repository and a management tool that aim at ensuring a consistent view over the IT infrastructure [16],[17]. These tool were designed to help maintain business-aware relation between business processes, users, and IT infrastructure reflecting configuration changes and their impact in business service.

BMC Atrium Orchestrator is comprised of specific tools that follow ITIL processes for Service Management, Problem Management and Service Automation, the goal is to provide an integrated Business Service Management environment to an organization**[18]**. This tool preforms like a workflow manager as it that allows the automation of routine operational procedures across an IT infrastructure.

BMC Dashboards for BSM & **BMC Analytics for BSM** are two platforms that help in providing a unified view over the an infrastructure key IT performance indicators **[19],[20]**.

Those indicators are fundamental in the operation and maintenance of an IT organization. Commonly, these indicators are scattered across several IT management tools and applications, making the task of delivering an overall view of performance and availability within an IT infrastructure a significant challenge.

3.3.2 CA

CA offers a portfolio of Enterprise IT Management solutions that aim at providing a platforms for managing IT infrastructures [21]. CA is currently owner of Spectrum, which was originally developed by Cabletron Systems, and was one of the first network management platforms commercially available. Next, follows a description of the management platforms and tools, per functional area, offered by CA that are designed to addresses the problems of managing a critical utility IT infrastructure.

CA NSM is a systems management platform designed to provide integration with other CA enterprise IT management platforms**[22]**. This platform provides in-depth event management along with performance reporting capabilities. Additionally it allows the creation of a service availability view that builds on correlating events together with the control and management systems and services.

CA Spectrum Automation Manager is a policy driven server management and automation platform**[23]**. This platform also provides configuration and change management. The automation features are designed to reduce costs and increase efficiency when managing critical operational environments.

3.3.3 EMC

EMC offers a portfolio of IT Management solutions that aim at providing a platforms for managing IT infrastructures [24]. Next, follows a description of the management platforms and tools, per functional area, offered by EMC that are designed to addresses the problems of managing a critical utility IT infrastructure.

IT Operations Intelligence is a platform that was designed to gather data from events, topology, and inventory across an IT infrastructure[25]. Using the information gathered to deliver centralized visibility into the entire IT infrastructure. It is comprised of several tools that provide automated, root-cause and impact analysis of networks, systems, and services.

3.3.4 HP

HP Business Technology Optimization [26], is an initiative from HP to address IT management necessities. The which they identified primarily as: Optimize allocation of IT resources based on business priorities, Automation of key processes across IT infrastructure, Measure IT effectiveness and efficiency.

Next, follows a description of the management platforms and tools offered by HP that are designed to addresses the problems of managing a critical utility IT infrastructure.

HP Operations Manager i 8.10 is a platform the helps the consolidation of IT infrastructure management operations [27]. In addition to systems and network consolidation it helps to consolidate operational processes to achieve better alignment with the business needs. This platform comprises a suite of products that address the challenges of managing IT operations.

HP Operations Smart Plug-ins (SPIs) are specific system plug-ins that provide intelligence and operational know-how to the management platforms[28].

HP Performance Manager is an analysis and visualization performance tool that provides operational insight on systems usage [29]. It performs system performance and bottleneck analysis, and allows baseline, forecast, and trend systems capacity.

HP Reporter is a management reporting solution that aggregates data collected by individual HP Operations Center software tools and platforms[30]. This software delivers historical reports and rich performance and availability data. That processed data is valuable management information that IT organizations can use for service level reporting and planning.

HP SiteScope provides availability and performance metrics over a distributed IT infrastructures [31]. The main distinctive features is that this is a agent-less monitoring platform. It was designed to provide a centralized view of an entire infrastructure without installing agents or software on production systems.

HP Universal Configuration Management Database (CMDB) platform by HP provides operators with a single view of the truth about the relations between infrastructure, applications and business services[32]. Like other platforms this software integrates with other HP IT management software platforms. This configuration management database supports business service management and ITIL-based initiatives.

3.3.5 IBM

IBM acquired a systems management company, Tivoli Systems, in 1996. The purchased Tivoli architecture was designed to allow the management of numerous remote locations and devices. Currently, Tivoli is part of IBM's Integrated Service Management business area. Next, follows a description of the platforms and tools under the Systems and Asset Management area that are designed to addresses the problems of monitors, controlling and optimizing the management of a critical utility IT infrastructure.

Tivoli Availability Process Manager provides coverage over IT components, applications with relation to their business impact[33]. Its focus is on providing the necessary tools to effectively diagnose and prioritize incidents. Gives IT operations mechanisms to determine and prioritize impact efficiently. Allows the creation of streamlined processes for IT operations staff. Relates existing SLAs and Operating Level Agreements, enabling a focused intervention by IT operations staff.

Tivoli Monitoring its the main monitoring platform from IBM it as a wide operating systems coverage, namely: AIX, HP Unix, IBM i family, Sun Solaris, Windows[34]. Its was designed to provide flexible workspace to enable system monitoring. It is aimed at detection and recovery from problems, in critical system resources, in an automated manner. It is designed to integrate with other composite application, event, network and service-level management solutions from IBM Tivoli.

Tivoli Performance Analyzer builds on Tivoli Monitoring to provide forecasting on resource utilization trends, enabling to change focus on monitoring of emerging problems[35]. Enables predictive trend analysis based on key operational metrics providing a view over system performance and capacity evolution over time. It as built-in metrics of specific distributed systems, including key performance indicators(KPIs) and thresholds that help IT operations staff managing the infrastructure.

Tivoli Configuration Manager is the configuration management platform from IBM**[36]**. It provides software distribution capability that enables efficient deployment of mission-critical applications to multiple locations from a central point. Includes an inventory module that enables automatic discovery of hardware and software configuration information. Additionally it can enforce adherence to your organization's policies by changing system configurations.

Tivoli Data Warehouse provides the repository for all systems management data and the starting point for all Tivoli reporting solutions[37].

3.3.6 Microsoft

Microsoft vision for IT management is the Systems Center initiative[38]. Next, follows a description of the platforms proposed by Microsoft that can address the problem of managing a critical utility IT infrastructure.

System Center Configuration Manager R2 platform provides a comprehensive solution for change and configuration management[39]. It collects hardware and software inventory, distributes and installs updates to software. Allow for monitoring compliance to a given configuration.

System Center Operations Manager 2007 R2 provides an end-to-end management capability over the IT environment as it delivers a comprehensive view of the health of an organization's IT environment[40]. This platform enables response to events via the detailed troubleshooting and best practices knowledge, included in the software package. It is designed to use application and operating system knowledge to identify operational problems. It provides a centralized management solution to monitor both Microsoft and non-Microsoft platforms and unified monitoring under a single tool.

3.3.7 IT Systems Management Platform Analysis

To create a basis for comparison and analysis we must first describe the features and properties that can serve to identify the strengths and weaknesses of these IT systems management platforms. Evaluation of these platforms is a subjective matter and naturally analysts are subject to a lot of marketing and business pressure. In this research we try to provide some insight on the characteristics that would enable the adoption of these platforms into a critical utility IT infrastructure.

On the technical side these platforms can be evaluated by large sets of parameters, which we arrange in sets to better summarize their coverage:

- **A** - Standards compliance and Interoperability. Grades the platform ability to adhere to standards, preventing vendor lock-in. Additionally, interoperability relates to the capability to operate in conjunction with legacy systems;
- **B** - Scalability. Relates to the degree to which the platforms can handle increasing number of managed hosts;
- **C** - Integration and Development capabilities. Relates to the openness of the platform to developer extensions;

- **D** - Monitoring independence. Relates to the system dependencies that are needed to deploy the management platform;

- **E** - Operational management of hosts. Relates to the capability the management platform has to effectively manage a given type of hosts, namely Windows OS hosts;

Apart from the technology features there are some other features that need to be taken into account when surveying these platforms. User sentiment and market impact are also valued when evaluating these platforms. Although not directly related to technology features of the product these metrics allow to establish comparisons related to the capacity and quality of the software producers. User sentiment usually is gathered via interviews with current users of the platforms and relates to factors like customer support, client engagement and vendor service capabilities. Market impact is more directed at analyzing vendor revenues, installed base, and geographic presence.

Table 3.1 sums up our qualitative evaluation of these platforms according to the proposed evaluation criteria. This evaluation was biased by the restricted operational scenario of the targeted critical utility IT infrastructure, based on the information provided by the vendors and included all the platforms from the vendors. The grade scale from 1 to 3 indicates limited - 1, regular - 2 and substantial - 3 technical capabilities.

Vendor	A	B	C	D	E	Total
BMC	2	3	1	1	1	8
CA	2	3	2	2	2	11
EMC	2	3	1	2	1	9
HP	3	3	3	2	2	13
IBM	3	3	2	2	2	12
Microsoft	3	3	3	3	3	15

Table 3.1: Comparative Table of the IT Management Platforms

3.4 Evaluation of Selected Platforms

We selected the two highest scoring vendors and chose two platforms, HP Operations Manager 8.10i and , to further analyze. For this analysis we studied the documentation and created an evaluation scenario which yields empirical insight to our evaluations.

3.4.1 HP Operations Manager 8.10i

HP Operations Manager for Windows (HPOM) is a distributed, client-server software solution designed to provide service-driven event and performance management of enterprise systems, applications, and services. HPOM enables management of distributed, heterogeneous, IT infrastructures and includes support for a broad range of Windows and UNIX systems and applications. HPOM monitors thousands of events occurring on all managed nodes and presents just the relevant information for a organization's needs.

3.4.1.1 Overview

HP Operations Manager software HP Operations Manager provides comprehensive event management, proactive performance monitoring, automated alerting, reporting and graphing for operating systems, middleware and applications. HP Operations Manager software consolidates an enterprise operations console for an entire IT infrastructure. Integration of events from the network monitoring solution and end-user experience monitoring provides IT operations team a comprehensive view of the managed environment.

HP Operations Manager for Windows software comprises three main components in a distributed architecture.

3.4.1.2 Operations Manager Console

The first component, the Operations Manager Console, provides the user interface for operations and administration. It is available as an Microsoft Management Console client or as a web browser interface.

To make use of the console each operator is provided with a specific user role based view, restricting what they see and what they can do within the managed environment. User roles include operational service views enabling operators to determine impact and root cause analysis associated with events.

Other operational functions are enabled by built-in tools, allocated by user role, that allow operators to run actions on managed systems, streamlining operational processes and optimizing operational efficiency. Additionally,a feature enables Operations Manager server to perform auditing and logging of operator activities.

Finally, built-in performance and reporting tools support monitoring and performance analysis of the managed environment.

3.4.1.3 Operations Manager Server

The Operations Manager server provides the business logic and manages a database which is used to maintain configuration information for the managed environment and the generated alerts and collected performance information.

The Operations Manager servers provide numerous functions, among them :

- Automated discovery of servers and applications infrastructure;
- Automated deployment of monitoring rules to managed nodes based on their application role;
- Receipt of events from the agents on the managed nodes, including event correlation, suppression and escalation;
- Consolidation of events from other tools, such as network monitors. Integration of events from systems monitored by third-party agents or agent-less technologies. This functionality provides a single normalized view of the managed environment;
- Forwarding of events to external notification systems and the ability to create, and synchronize, incident tickets in help desk management systems;
- Addition of resolution guidance information into events and the provision of operator-guided actions for issue resolution;
- Integrated scheduled and operational maintenance modes for managed systems to prevent operations staff from seeing false alarms during authorized interventions;
- Scalable, and flexible deployment architectures including support for high-availability cluster architectures and disaster tolerant distributed architectures with multiple Operations Manager servers.

3.4.1.4 Operations Manager Agents

HP Operations Manager agents are installed on managed hosts collecting, aggregating, and correlating monitoring information from a variety of information sources. These agents are extensible and customizable allowing incorporation of any monitoring source not included in the out-of-the-box monitoring policies. Additionally, agents collect and analyze performance data and can use historical patterns to establish performance baselines.

Note that HPOM agents are autonomous and can undertake automated corrective actions without indication from the Operations Manager server. By using filtering, duplicate suppression and correlation, the agents manage by exception only forwarding actionable events to the Operations Manager server.

Finally, Smart Plug-Ins (SPIs) provide packaged application management for Operations Manager. SPIs include application-specific auto-discovery, pre-defined monitoring policies, actions, tools and detailed performance data collection. Core Smart PlugIns are included with HP Operations Manager for Windows and provide coverage for systems and applications. Each Operations Manager Agent includes an Operating System SPI for the relevant OS (Windows, Linux, UNIX).

3.4.2 Microsoft System Center Operations Manager 2007 R2

Microsoft System Center Operations Manager 2007 R2 (SCOM) provides the end-to-end management capability over the IT environment. SCOM provides a comprehensive view of the health of an organization's IT environment. SCOM enables response to events via the detailed troubleshooting and best practices knowledge included in the software package, especially in Windows environments. SCOM can use application and operating system knowledge to identify operational problems.

This platform provides a centralized management solution to monitor both Microsoft and non-Microsoft platforms. It provides unified monitoring under a single tool as data is aggregated across environments to present one picture of performance and availability.

3.4.2.1 Overview

An Operations Manager 2007 infrastructure is composed of core components and a set of optional components. This section describes these components and features. Figure3.1 gives a high level description of key SCOM components.

3.4.2.2 Required Server Roles and Components

The basic unit of functionality of all Operations Manager 2007 implementations is the management group. It consists of the Operations Manager database, the root management server, the Operations console, and one or more agents that are deployed to monitored computers or devices are the base components of a management group.

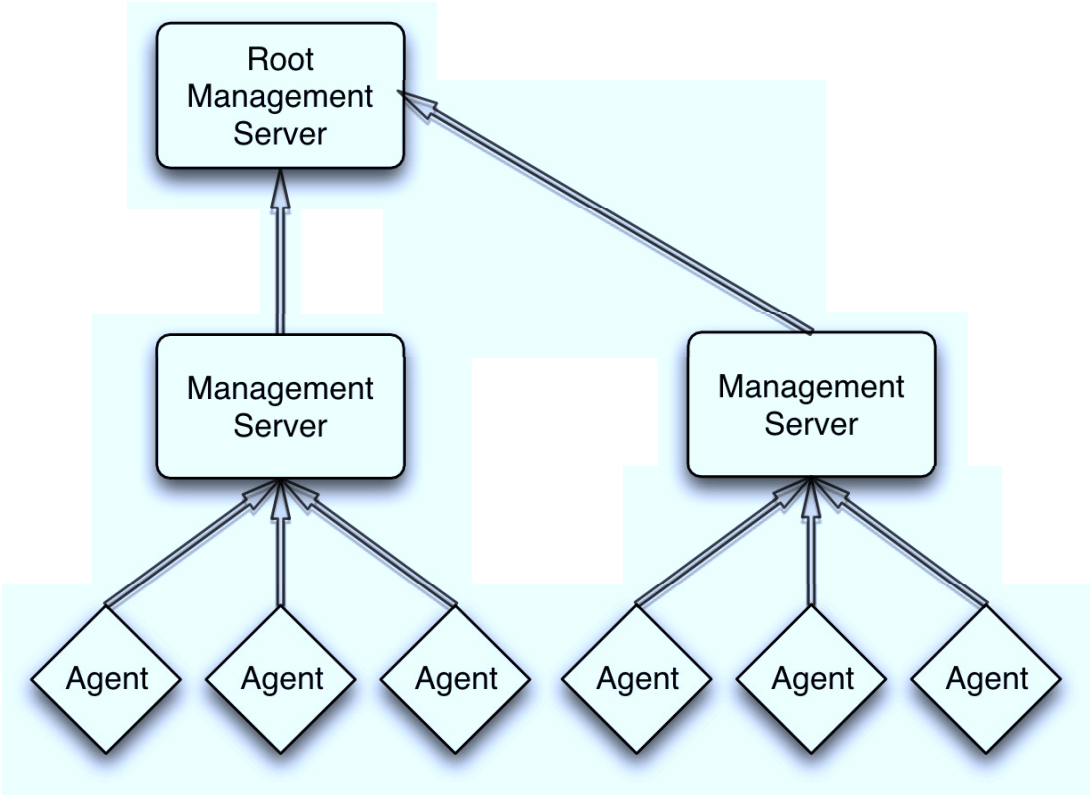

Figure 3.1: Systems Center Operations Manager 2007 R2 Architecture

Operations Manager Database

The Operations Manager database is the first component to be installed in all management groups. This database holds all the configuration data for the management group and stores all the monitoring data that has been collected and processed by the agents.

Because only one Operations Manager database can be in a management group, it must be functional for the management group to function. To mitigate the single instance of the Operations Manager database from being a single point of failure, the Operations Manager database can be placed in a Cluster service fail-over cluster. In addition, log shipping can be configured so that current operations data and configuration information can be sent to another server that is hosting a duplicate copy of the primary Operations Manager database. Should there be a failure in the primary database, the duplicate can be updated and switched to.

Root Management Server

The root management server (RMS) is a special type of management server in a management group. Only one RMS can be active per management group at a time. In brief, the RMS is the primary point for administering the management group configuration, administering and communicating with agents, and communicating with the Operations Manager database and other databases in the management group.

The RMS hosts the System Center Data Access service and the System Center Management Configuration service. These services run only on the RMS. The System Center Data Access service provides secure access to the Operations Manager database for all clients, including the Operations console, Operations shell, and Web console. The System Center Management Configuration service is responsible for calculating and distributing the configuration of all management servers, agents, and management packs.

Like the Operations Manager database, the RMS role can be installed into an fail-over cluster to make it highly resilient to primary server outages. In addition, other management servers in the management group can be promoted to the role of RMS.

Agent

An Operations Manager 2007 agent is a service that is deployed to a computer to be monitored. On the monitored device, an agent is listed as the System Center Management service. Every agent reports to a management server in the management group. This management server is referred to as the agent's primary management server. Agents watch instrumentation data sources on the monitored device and collect information according to the configuration. When the state of a monitored object changes or other criteria are met, an alert can be generated from the agent. The agent is also able to calculate the health state of the monitored object and report back to the management server.

Agents also have the ability to take many different types of action to help diagnose issues or correct them. By feeding health data to the management server about the monitored device, the agent provides an up-to-date picture of the health of the device and all the applications that it hosts.

It is possible to monitor devices in an agent-less fashion. In this case, a management server pools the monitored device for information.

Operations Console

The Operations console provides a unified user interface for interacting with Operations Manager 2007. The Operations console provides access to monitoring data, basic management pack authoring tools, Operations Manager 2007 reports, all the controls and tools necessary for administering Operations Manager 2007, and a customizable workspace.

For a user to access the Operations console, the user account must be assigned to an Operations Manager 2007 user role. A user role is the combination of a scope of devices that access is granted to and a profile that defines what the role can do within its defined scope. Role-based security is enforced in the Operations console so that Operations Manager administrators can define what any given user can see in the console and what actions the user can take on those items.

Management Packs

Management packs contain an application's health definition as defined by the application developers. They enable the agent to monitor the health of an application, generate alerts when something of significance goes wrong in the application, and take actions in the application and its supporting infrastructure to further diagnose the application or restore it to a healthy state. Without an application, operating-system, or device-specific management pack, Operations Manager 2007 is unaware of those entities and is unable to monitor them.

3.4.2.3 Optional Server Roles and Components

These additional server roles extend the functionality of a management group.

Management Server

A management server is used primarily for receiving configurations and management packs from the RMS and distributing them to the agents that report to the management server. It does not perform any of the special functions of the RMS, but can be promoted to the RMS role if the primary RMS fails. Besides increasing scalability, introducing additional management servers in a management group for fail over scenarios.

The management server can also be used for remote monitoring purposes, for example: URL monitoring and cross-platform monitoring.

Gateway Server

Operations Manager 2007 requires that agents and management servers authenticate each other and establish an encrypted communication channel before they exchange information. Kerberos is the default authentication protocol. Since our scenario is implemented on top of a logical Windows domain using the default authentication protocol, Kerberos, mutual authentication is guaranteed by default for agent and management server communications. When agents and management servers are not within the same Kerberos trust boundary, certificate-based authentication mechanisms must be used. In this situation, a certificate must be issued and maintained for those agents and the management servers to which they report.

An Operations Manager 2007 gateway acts as a proxy for agent communications. The gateway server is placed within the trust boundary of the agents (which can be a logical domain), and all the agents communicate with it. Then the gateway server, through the use of its computer certificate, performs mutual authentication with the management server and forwards the agent-to-management server and management server-to-agent communications along. This then requires only one certificate for the management server and one for the gateway.

Multiple gateway servers can be installed in a management group for the purposes of scalability and fail-over.

Reporting Data Warehouse

The Reporting Data Warehouse stores monitoring and alerting data for historical purposes. The management servers write their data to the Data Warehouse at the same time it is written to the Operations Manager database, so the reports generated always contain the most up-to-date data.

The Reporting Data Warehouse can receive data from multiple management groups, thereby allowing for an aggregated view of data in your reports.

Reporting Server

Operations Manager Reporting Server it is responsible for building and presenting the reports from data queried from the Reporting Data Warehouse. All reports are accessed in the Operations console, so access to reports is controlled via role-based security.

Audit Collection Services

Audit Collection Services (ACS) collects and stores events from the Security Event Log on monitored computers, events are stored in a separate database, the ACS database. ACS collects all events written to the Security Event Log on computers that the ACS Forwarder is enabled on. Events are forwarded from monitored computers to the ACS Collector, which runs on a management server, which then processes them and writes them to the ACS database. The events are transmitted in an encrypted, near real-time fashion from the forwarders to the collector. A separate component, ACS Reporting, is then used to generate reports from the stored ACS data.

A key to using ACS effectively is the development of a solid Windows Audit Group Policy that is implemented as a domain Group Policy or a specific computer object collection (i.e., organizational unit) Group Policy.

ACS Forwarder

The ACS Forwarder is embedded in the Operations Manager 2007 agent, so no separate deployment or configuration is required. The ACS Forwarder appears as the Audit Forwarder service and is disabled by default. The ACS Forwarder on an individual computer or on groups of computers can be remotely enabled via the Operations console.

ACS Collector Server

The main purpose of the ACS Collector server is to collect, filter, and pre-process all the Windows security log events for insertion into the database. Because the ACS collects all security events in near real-time, vast amounts of data enters the system from the forwarders. The filtering mechanism at the collector allows you to specify which events you want written to the ACS database for long-term storage.

ACS Database

After the data has been pre-processed by the ACS Collector server, it is written to its ACS Database. Because it is a standard SQL database, it can be clustered for high-availability. To accommodate the one-to-one relationship between collectors and databases, one can create multiple ACS Databases on a single server.

ACS Reporting

The ACS Reporting server as a number of pre-configured reports. But it depends on the organization's needs how the audit information can be used. Intrusion detection via statistical anomaly behavior can be envisioned on top of the reporting services provided by ACS Reporting.

Proxy Agent

Operations Manager 2007 has the ability to monitor network devices, computers that are not running a Windows operating system, and computers without agents. To accomplish monitoring of these hosts another computer that has an agent installed will perform the monitoring remotely, a proxy agent function. The agent that is acting as a proxy for monitoring other devices is a standard Operations Manager agent, but is configured differently.

Operations Manager 2007 Command Shell

The Windows PowerShell is a command-line interface for use on Windows Server 2003, Windows Server 2008, Windows XP, and Vista operating systems. This interface was developed for use by system administrators for automating tasks.

Cross-Platform Monitoring (UNIX-based or Linux-based Computers)

Operations Manager 2007 R2 management servers and gateway servers can monitor UNIX and Linux computers.

In cross-platform monitoring, the system center management service on the management server or gateway server runs all the monitoring intelligence. The monitoring system center management service communicates with the monitored computer through a WSMAN layer[13] that is on both the management server and the computer being monitored. It is a prerequisite that the WSMAN layer be installed on the monitored computer. SSH can be used for installing the WSMAN layer or performing diagnostics.

3.4.2.4 Management packs

Operations Manager can work with a variety of instrumentation. It can use, namely: Windows events, Windows performance counters, Windows Management Instrumentation

(WMI) events, WMI performance data, Log file events, Simple Network Management Protocol (SNMP) traps. The mechanism that orchestrates how monitoring is preformed is a Management Pack (MP). The management pack describes an application and directs Operations Manager how to monitor it. A management pack is a xml document which is divided into several sections and must adhere to a specific schema.

3.4.3 Evaluation

We created a testbed scenario in order to evaluate these tools in a operational environment. The scenario consisted of several hosts organized in a logical Windows Domain, we called it SCADA.local. Table 3.2 describes function and configuration per machine.

Host	OS	Configuration
DC000001	Windows 2008 Server Standard	Domain controller, Network Services
SV000001	Windows 2003 Server Standard	Microsoft System Center Operations Manager 2007 R2
SV000002	Windows 2003 Server Standard	HP OpenView Operations Manager 8.10i
SV000003	Windows 2008 Server Standard	Monitoring target
DV000001	Windows 2003 Server Standard	Visual Studio 2008, MS SQL 2008
WS000001	Windows XP SP3 // Embedded	Monitoring target, Host for HP OpenView Operations Manager 8.10i agent, Host for System Center Operations Manager 2007 R2 agent

Table 3.2: Testbed Configuration Per Machine

Our evaluation was based on the process of configuration of the management platforms. Depending on the platform we followed its, extensive, documentation in order to configure some monitoring scenarios.

We also evaluated the global impact of having agents for the management platforms installed in a production system.

We came across some significant challenges when trying to relate monitoring of a critical control system to common application monitoring. In the studied platforms agents and monitoring ability rely on user mode performance counters, activity logs, WMI pooling or traps and Registry events. None of the tested platforms allowed for a configurable in depth analysis of an application's behaviour without major drawbacks.

On HP OpenView Operations Manager 8.10i the dependency of the whole platform on SPIs is critical. The major difference in relation to Microsoft System Center Operations Manager 2007 R2 was the nonexistence of documentation on how to develop SPIs, although it possesses some extensive automation and integration capabilities. Additionally, this platform when managing a host via an agent installs numerous extra OS components that in turn add to the complexity of the managed host, in some control systems installing such an agent is simply not supported.

On the other hand, Microsoft System Center Operations Manager 2007 has available an extensive documentation library, the most complete of all surveyed vendors. But the Business Service Management capabilities of System Center 2007 make any attempt to model an application and creating a management pack a significant challenge, specially if the modeler is not the developer of the application.

Both vendors rely on the software application developers to create the Management Packs and SPIs to enable integrated management capabilities. But SMNP[12] and WS-MAN[13] support, in both platforms, adds to the monitoring capabilities via standardized methods.

In summary, both platforms have immense capabilities while addressing the monitoring of a large-scale distributed system. However their dependence on the agents is critical. In both platforms host agents behave like *"fat clients*", and although our claims have not yet been tested in a real control system host we firmly believe that the overhead of such agents operations in a real control system would turn prohibitive such a monitoring and management scenario.

In Chapter 4 we propose to investigate the management mechanisms of the Windows OS, the COTS operating system used in the construction of these critical utility IT Infrastructures.

In Chapter 5 we propose to investigate a lightweight monitoring solution for the Windows OS, the COTS operating system used in the construction of these critical utility IT Infrastructures.

Chapter 4

Windows Management Architecture

In this chapter we will describe the process of managing Microsoft Windows operating systems. We start by looking at the management mechanisms present in the OS in order to better understand how to integrate this features in a IT systems management platform. Keeping in mind that a critical utility IT infrastructure has to support control systems with stringent operational requirements.

There are several management and configuration mechanisms for a Windows operating system. The essential parts of any windows system are the Registry and Windows Management Instrumentation, they play a key role in management, configuration and control of a Windows operating system.

These mechanisms are important because IT management platform agents use them to monitor and manage systems. In summary, they represent management mechanisms available to developers, which are in turn invoked by IT platform agents to manage a designated host.

4.1 The Registry

The registry is a hierarchical database that stores and manages data. This data is structured in a tree format. Each node in the tree is called a key. Each key can contain sub-keys and data entries (values).

The registry plays a central role in the configuration and control of a Windows system. Far from simply static data stored on the hard disk the registry it is also a view into various in-memory structures maintained by the Windows executive and kernel.

Applications store distinct types of data in registry entries. Usually, programs use Win32 APIs to read data from the registry. The developer specifies a registry location entry and the API returns the value of the entry. Programs can also use the standard APIs to add and delete registry content, and to change the values of registry entries. After it retrieves and reads the data in the value of an entry, each program interprets the data and implements its result independently, depending on how the program is written. A file location stored in a registry entry might tell a program where to find a given file.

Windows operating system components use the registry in the following ways:

Setup Windows setup program and other setup programs add configuration data to the registry. For example, new information is added when you install a new SCSI adapter or a specific controller.

Recognizer Upon system start the hardware recognizer places hardware configuration data in the registry. This data includes a list of hardware detected in your system. Hardware detection is done by the hardware recognizer, Ntdetect.com, and the Windows kernel, Ntoskrnl.exe, programs.

Kernel During system starts, the kernel extracts information from the registry, such as which device drivers to load and their load order. The kernel also stores information in registry.

Drivers Device drivers send and receive configuration data from the registry. A device driver must report the system resources that it uses, such as hardware interrupts and DMA channels, this information is then added to the registry. Given that programs are so variable, it is very difficult to predict how a specific program will interpret the registry data.

4.2 Windows Management Instrumentation

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-based Enterprise Management (WBEM), which is an industry initiative to develop a standard interface for accessing management information in an enterprise environment. WMI uses the Common Information Model (CIM), one industry standard, to represent systems, applications, networks, devices, and other managed components[41]. CIM is developed

and maintained by the Distributed Management Task Force (DMTF)[42]. WMI is the instrumentation mechanism through which nearly all Windows resources can be accessed, configured, managed, and monitored. Figure4.1shows in high level architecture of WMI.

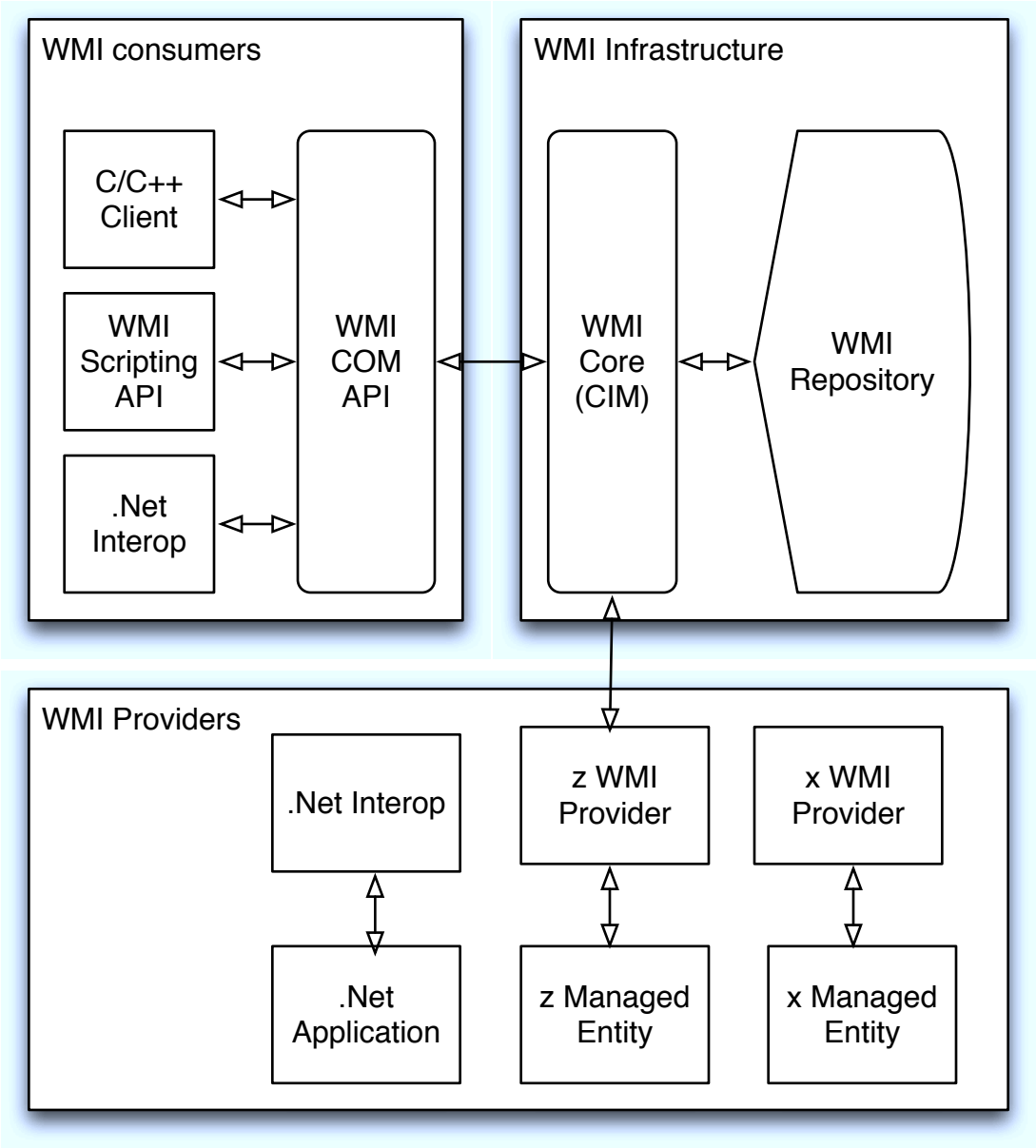

Figure 4.1: WMI Architecture

To grasp the power and breadth of WMI, consider managing and monitoring several Windows workstations and servers. To effectively manage the set of machines an operator would have to have probably used numerous graphical administrative tools to manage resources, such as disks, event logs, files, folders, file systems, networking components,

operating system settings, performance data, processes, registry settings, security, services, users, groups, among other details.

Graphical tools provide a functional management solution, but prior to WMI, all Windows graphical administrative tools relied on Win32 APIs to access and manage Windows resources. This was the only way to programmatically access Windows resources before WMI. This unwanted feature left Windows operator without an effective way to automate and audit system administrative tasks using popular scripting languages, like common administration paradigms of Unix or Linux platforms. WMI provides a consistent model and framework through which Windows resources are described and exposed.

Using scripting environments operators can write scripts to automate the several aspects of enterprise systems, applications, and networks management, namely:

- Server managers can deploy scripts to retrieve performance data, manage event logs, file systems, printers, processes, registry settings, scheduler activity, services, shares, and numerous other operating system components and configuration settings.
- Network managers can deploy scripts to manage network services such as DNS, DHCP, and SNMP-enabled devices.
- Security managers can perform health monitoring. Using WMI event subscriptions to monitor and respond to event log entries as they occur, file system and registry modifications, and other real-time operating system changes.
- Application managers can manage WMI enabled applications.

4.3 Windows Securable Objects

The basic unit of security management in Windows is a securable object. Simply put, a securable object is an object that can have permissions applied to it. The different types of securable objects in a Microsoft Windows include:

- Files
- Directories
- Registry keys
- Kernel objects (events, semaphores, mutexes)

- Services
- Threads
- Processes
- Firewall Ports
- Window stations and desktops
- Active Directory objects

These objects are subject to modification by the normal operation of the Operating System and its applications. These are points of observation to the behavior of the whole Operating System, can be related to functional patterns, and can used to describe faults, errors and failures of the OS and its applications.

Chapter 5

Monitoring COTS Control Systems

To be able to describe the system behavior on meaningful operating scenarios we need to monitor a given system under operational stress. One mechanism provided by Windows Operating Systems is called Event Tracing for Windows (ETW) and we can build on that mechanism to preform detailed analysis on the operating system behavior.

5.1 Event Tracing

Event tracing signifies collecting meaningful events from parts of the operating system of interest to our research. The ETW architecture allows for dynamic and efficient trace and event management.

Event tracing for Windows (ETW) is a tracing mechanism provided by the Windows Operating System. ETW supports user-mode programs and kernel-mode device drivers. The logging mechanism uses per-processor buffers that are written to disk by a separate writer thread. ETW events include metadata, message strings, and structured data payloads for processing of event data.

Additionally, ETW can enable or disable tracing features dynamically, which makes it possible to perform detailed tracing in production environments without requiring system reboots. This is of great value to us since one of our future goals is to preform detailed analysis of the Windows OS in a real environment with critical control systems.

ETW is one of the key instrumentation technologies on Windows platforms. Next we present an overview of ETW architecture and usage model.

The core architecture of ETW is illustrated in Figure 5.1. As shown, there are three main types of components in ETW: event providers, controllers and consumers. Additionally,

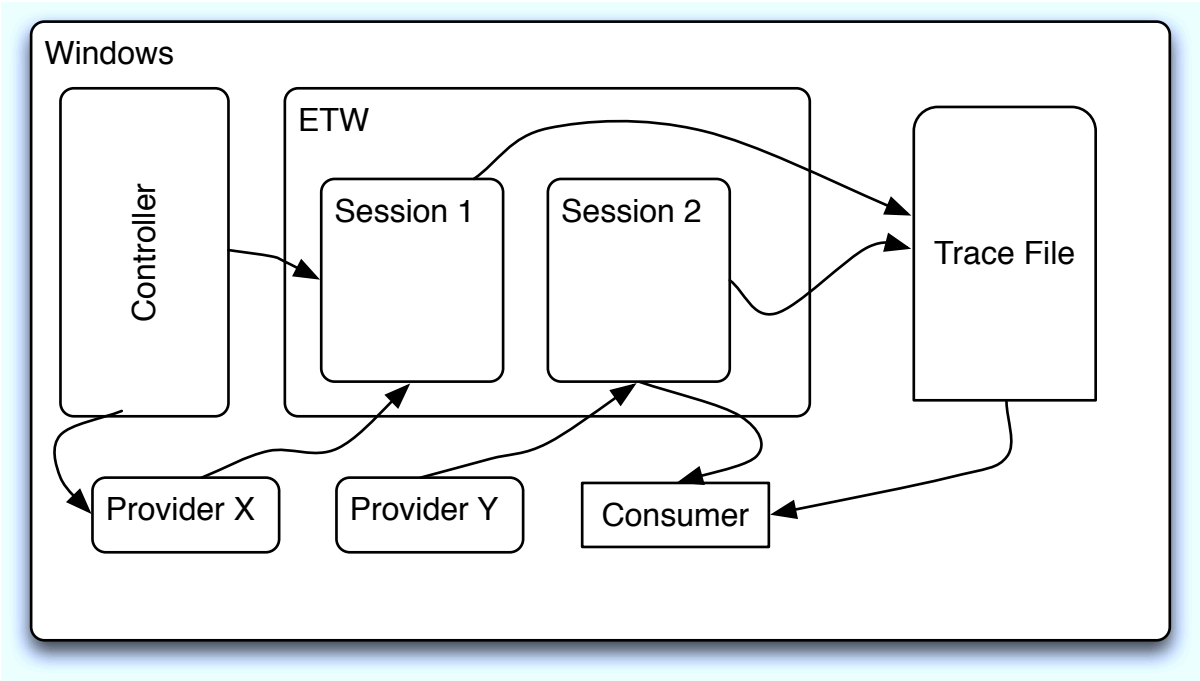

Figure 5.1: ETW Architecture

event trace sessions are responsible for buffering, logging and creating a trace file. There are several logging modes available for ETW sessions. For instance, a session can be configured to deliver events directly to consumer applications or to overwrite a circular log file. A separate writer thread created for each session flushes events to a file or to real-time consumer applications. To enable higher performance per-processor buffers are used to eliminate the need for locks while logging.

An event provider is a logical mechanism that writes events to ETW sessions. An Event is just any activity of a given significance can be an event. As explained above an event provider can be a user-mode application, a managed application, a driver, or other program. There is one requirement however, the event provider must register a provider ID with ETW through the registration API. A provider first registers with ETW and then writes events from within the code by invoking the ETW logging API. When a provider is enabled by the ETW controller application, calls to the logging API send events to a specific trace session designated by the controller.

An event consists of a fixed header that includes event metadata and additional variable user-context data. Due to the growing event instrumentation in many OS and development components, even a common simple application will already contain several components that are event providers. When an event is logged to a session, ETW adds a extra data items along with the user-provided data, namely: timestamps, process ID, thread ID, pro-

cessor number and CPU usage data of the logging thread. These items are recorded in the ETW event header and passed on to event consumers together with the variable event content given by the provider. These data fields can be essential to consumers to preform appropriate analysis.

A controller manages, starts or stops, ETW sessions and can enable providers to the sessions. In some debugging scenarios a controller tool is invoked, as needed, to collect in-depth traces. In contrast, and of special importance to this research, for events such as admin-targeted events providers are enabled automatically by the event log service when they register. From an access control point of view a controller must have a specific ETW permission on a Windows system to be able to control sessions.

A consumer is a program that can read log files or, more importantly for critical control systems, listens to a session's real time events and while processing them. Event consumption is callback mechanism where a consumer registers an event callback, which the ETW mechanism calls event by event. This enables events being delivered to the consumer in chronological order.

The ETW architecture allows for sessions and providers to coexist in different conceptual spaces. A controller is responsible for starting and stopping ETW sessions and enabling providers to sessions. A controller can choose to enable a group of providers to a session, disable some of them after a while, and enable another provider to that same session later. Sessions operate in the kernel and are not statically linked to providers. Likewise, providers are not aware of which sessions are logging their events.In a generic system there can be large scale applications and services that are providers, controllers, and consumers at the same time. This separation of providers and trace sessions makes tracing immune to application problems such as crashes or hangs. Events can be used by developers, IT administrators, and management tool developers for debugging, monitoring, diagnosis, and capacity planning.

5.2 Analysis Techniques

A kernel trace can contain, and usually contains, much more information than one is interested in. We studied Windows SDK[43] and Windows Performance Analysis Tools [44] to gain insight on the Windows architecture and on the performance impact of using ETW for monitoring critical control systems.

One option that a researcher does have is to build its own event trace consumer and perform

treatment of events in real-time. The overhead for that treatment depends on the number of events consumed and the extra processing by event. In special cases, where specific applications are ETW producers, real-time monitoring can be achieved with very low overhead.

One other option in analyzing an event trace is using a trace file, (*.etl) which is just the output buffers produced by the kernel trace session written to a file. This data is raw no preprocessing is done on the file and no metadata is associated with it, since it comes directly from the kernel. This feature allows for efficient event tracing but it also, to some extent, impairs real-time system wide monitoring.

Before off-line analysis may take place we must use a merge tool, xperf [45]. Xperf will merge metadata to the trace. This merge step must happen on the system where the trace was taken and this process requires core trace processing components to do a lot of processing on the raw trace data. This includes mapping process IDs (PIDs) to file and process names, mapping addresses to file names, loading symbols for address, unifying stacks. Care must be taken when trying to use these mechanisms on production environment systems, specially on control systems where timeliness requirements are strict.

The usual off-line analysis methodologies based on events can be categorized into the following techniques:

- Scanning through the event file to find specific events or a simple pattern of known events.

- Statistical analysis can be done by studying event distribution or simply by event counting. Certain occurrences of events (Page Faults, for example) provide additional insight into system behavior.

- A state machine approach can be constructed on a given set of events. Such a state machine would prove invaluable in simulations of the control environment and in the construction of a operational profile. This is possible since the large majority of core OS activities are instrumented with ETW events. Specific Kernel, OS traces can be used to build a state machine for resource tracking (i.e, keeping track of scheduler, memory, I/O activities, TCP/IP activities).

- Distributed control systems consist of several components interconnected via network. They span multiple machines, each serving a distinct role. Instrumenting control requests at distinct systems is one approach to obtain end-to-end visibility of related events. It is possible to instrument applications to record activities along

with the unique ID for a given request. Upon event processing, events that correspond to the request ID can be correlated and progress can be evaluated. Following this approach is fairly simple to isolate a group of typical requests, through a statistical analysis, that serve as an application baseline. Therefore enabling end-to-end monitoring.

5.3 Windows OS Event Providers

OS event providers are components of the OS and its applications that have been instrumented to generate events.

When doing performance or baseline analysis researchers have to carefully choose which providers have the desired relevance. Such a task should have solid theoretical foundations, but nonetheless it should result from an empirical study of the environment, systems and applications.

To better illustrate our claims next follows a small subset of default enabled event providers:

...

Microsoft-Windows-User-PnP

Microsoft-Windows-DiskDiagnostic

Microsoft-Windows-Firewall

Microsoft-Windows-DiskDiagnosticDataCollector Ntfs

Microsoft-Windows-IPBusEnum

Microsoft-Windows-StartupRepair

Microsoft-Windows-UAC-FileVirtualization Microsoft-Windows-GroupPolicy

Microsoft-Windows-Kernel-General

Microsoft-Windows-Kernel-PnP

Microsoft-Windows-Resource-Exhaustion-Detector

Microsoft-Windows-TPM-WMI

Microsoft-Windows-HttpEvent

Microsoft-Windows-Kernel-WHEA

Microsoft-Windows-ResourcePublication

Microsoft-Windows-MemoryDiagnostics-Schedule

...

Of particular importance to our research is the kernel instrumentation. The kernel provider exposes large amounts of information, and the event generation can be controlled via flags and/or groups. Kernel provider flags enable/disable the logging of a kernel event type. For example, if PROC_THREAD is used in the definition of a session, events will be logged for process creation or deletion. Next, in table 5.1, the default kernel flags for Windows 2008 Server.

Flag Name	Function
PROC_THREAD	Process and Thread create/delete
LOADER	Kernel and user mode Image Load/Unload events
PROFILE	CPU Sample profile
CSWITCH	Context Switch
COMPACT_CSWITCH	Compact Context Switch
DISPATCHER	CPU Scheduler
DPC	DPC Events
INTERRUPT	Interrupt events
SYSCALL	System calls
PRIORITY	Priority change events
ALPC	Advanced Local Procedure Call
PERF_COUNTER	Process Perf Counters
DISK_IO	Disk I/O
DISK_IO_INIT	Disk I/O Initiation
FILE_IO	File system operation end times and results
FILE_IO_INIT	File system operation (create/open/close/read/write)
HARD_FAULTS	Hard Page Faults
FILENAME	FileName (e.g., FileName create/delete/rundown)
SPLIT_IO	Split I/O
REGISTRY	Registry tracing
DRIVERS	Driver events
POWER	Power management events
NETWORKTRACE	Network events (e.g., tcp/udp send/receive)
VIRT_ALLOC	Virtual allocation reserve and release
MEMINFO	Memory List Info
ALL_FAULTS	All page faults including hard, copy on write

Table 5.1: Flags Per Function

A kernel provider group is a set of flags of importance for a given component or area of

interest. For example, the group Latency consists of the necessary flags to provide information necessary to do latency related analysis. Multiple groups and flags can be enabled for the same trace. Next, in table 5.2 follow the default kernel groups for a Windows 2008 Server.

Group Name	Enabled Flags
Base	PROC_THREAD + LOADER + DISK_IO + HARD_FAULTS + PROFILE + MEMINFO
Diag	PROC_THREAD + LOADER + DISK_IO + HARD_FAULTS + DPC + INTERRUPT + CSWITCH + PERF_ R + COMPACT_CSWITCH
DiagEasy	PROC_THREAD + LOADER + DISK_IO + HARD_FAULTS + DPC + INTERRUPT + CSWITCH + PERF_ R
Latency	PROC_THREAD + LOADER + DISK_IO + HARD_FAULTS + DPC + INTERRUPT + CSWITCH + PROFILE
FileIO	PROC_THREAD + LOADER + DISK_IO + HARD_FAULTS + FILE_IO + FILE_IO_INIT
IOTrace	PROC_THREAD + LOADER + DISK_IO + HARD_FAULTS + CSWITCH
ResumeTrace	PROC_THREAD + LOADER + DISK_IO + HARD_FAULTS + PROFILE + POWER
SysProf	PROC_THREAD + LOADER+ PROFILE
Network	PROC_THREAD + LOADER + NETWORKTRACE

Table 5.2: Flags Per Group

5.4 Kernel Trace Analysis

Windows OS features hundreds of event providers from various components and applications. From the core OS ETW events available there are several analysis techniques that can be used to provided needed insight on a scenario with stringent timeliness requirements. Individual events indicate run-time changes in the core OS, but together with context-sensitive analysis methods, they can be used to add insight into patterns and problems in resource usage. This tracing mechanism enables, for example, the construction of state machine baselines that can be used by monitoring functions to assert deviations from normal behavior. Next follows the description of the information that can be extracted by analyzing a kernel trace. Other types of information can be extracted, but we will focus on the information that will allow us to monitor, manage and build better control systems in critical utility IT infrastructures.

5.4.1 Process, Thread, Modules, Process Counter Events

A thread is a basic unit of execution on the Windows OS, and a process acts as a container for threads. Each process, and thread, is assigned an unique ID while it is running. Processes and threads generate two types of events: *Start events*, generated when a process/thread starts, and *End events*, when a process/thread terminates. The event payload for process/thread has several details about the process. For reference, table 5.3 displays a XML dump of a process end event.


```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Guid="{9e814aad-3204-11d2-9a82-006008a86939}" />
<EventID>0</EventID>
<Version>1</Version>
<Level>0</Level>
<Task>0</Task>
<Opcode>1</Opcode>
<Keywords>0x0</Keywords>
<TimeCreated SystemTime="2009-10-09T12:54:25.915493800Z" />
<Correlation ActivityID="{00000000-0000-0000-0000-000000000000}" />
<Execution ProcessID="4" ThreadID="108" ProcessorID="0" KernelTime="195"
UserTime="0" />
<Channel />
<Computer />
</System>
<EventData>
<Data Name="ProcessId">0x4</Data>
<Data Name="TThreadId">0x86C</Data>
</EventData>
<RenderingInfo Culture="pt-PT">
<Opcode>End</Opcode>
<Provider>MSNT_SystemTrace</Provider>
<EventName xm-
lns="http://schemas.microsoft.com/win/2004/08/events/trace">Thread</EventName>
</RenderingInfo> <ExtendedTracingInfo
xmlns="http://schemas.microsoft.com/win/2004/08/events/trace">
<EventGuid>{3d6fa8d1-fe05-11d0-9dda-00c04fd7ba7c}</EventGuid>
</ExtendedTracingInfo>
</Event>
```


Table 5.3: XML dump of *Process End* Event

Without going into much detail, every process and thread that is active during event collection can be traced using process and thread events. These details on processes and threads

are the starting point when establishing a state machine approach for a system behavior. For example, when modeling a state machine for a given system behavior, it could be valuable to keep a list of active processes and threads along with a list of terminated processes or threads.

Module, *library or image events* correspond to the loading, and unloading, of module files to, and from, the process address space. These events allow for the tracking of loaded modules, libraries and the mapping of addresses within a process. This event payload contains details such as: module address base, size, name of the binary file. These events are required for decoding call-stacks, again extremelly important when considering a state machine approach for a system behavior study.

Process counter events record in its payload a details regarding the process execution statistics over the lifetime of the process. These counters describe process behavior in respect to memory utilization. Not so useful for state machine approach, but still valuable for system wide analysis of memory usage.

5.4.2 Context Switch and Interrupt Service Routine Events

Context switch events are logged on every thread switch. This information can be used to a time-line with relation to which threads have been running and for how long. *Context switch event* details contains old and new thread IDs, old and new thread priorities, wait reason and wait time. Many situations may lead to a context switch, namely: blocking on kernel synchronization objects, preemption by a higher priority thread, changes in thread affinity. Together with call-stacks mechanism, *Context switch events* allow in-depth analysis on reasons that lead to threads getting preempted.

Interrupt Service Routine (ISR) events details record entry time, routine address, ISR vector and ISR return value. Deferred procedure calls(DPCs) are kernel-mode functions executed at elevated interrupt-level execution mode. DPCs together with ISRs are critical components of a Windows driver. These *DPC & ISR events* can be used to monitor behavior of drivers and kernel-mode components. Used together with module event details, the routine address can be compared for determining which kernel component responsible for those DPC and ISR events.

In a state machine approach, combining *Context switch, DPC & ISR event* details enables an accurate accounting of system behavior and CPU utilization. With these mechanisms it is possible to analyze what the CPU was doing at any given time and what piece of code it was executing.

5.4.3 Memory Events

Memory events can be: *Page Fault events* or *Hard Page Fault events*. A *Page Fault event* payload contains the address of the virtual memory for which a page fault has occurred and the instruction pointer that caused it. Accordingly, a *Hard Page Fault event* requires disk access to occur and typically has a considerably larger impact on performance. *Hard Page Fault event* payload details consist of file key, offset and thread ID, which identifies the thread causing the page fault. This enables the correlation of *Page Fault events* to threads and processes, when considering a state machine approach.

5.4.4 Network Events

Network events can be logged when network activities occur at TCP/IP and UDP/IP layers. *TCP/IP events* are logged on the following actions by the network drivers: Send, Receive, Disconnect, Retransmit, Reconnect, Copy, and Fail. The details contain the packet size, source and destination IP addresses, ports, the originating process id for *Send type events* and the target process id for *Receive type events*. This means that *Network events* can be related to a process, adding considerable insight to a baseline analysis or the construction of a state machine emulator for a given system.

5.4.5 Registry Events

Registry operations are instrumented with ETW, therefore *Registry events* can be attributed to processes and threads. *Registry events* can be extremely useful in characterizing Registry access patterns. The *Registry event* payload details also the return status of registry operations, which can be used to monitor registry operation failures and effectively describe the utilization, by any process, of the Registry.

5.4.6 Sample-Based Profile Events

Profile events allow characterizing where CPU spent its time in execution. *Sample-based profile events* makes Windows kernel turn on profiling interrupts, which causes *Profile events* to be logged from each processor at a fixed rate. The *Profile event* payload details consists of the thread id of the thread running on a given processor and the value of the instruction pointer register at the time of the profiling interrupt. Together with *Process* and *Thread events* it is simple to generate a per-process CPU usage report, and using *Image load*

events it is possible to trace CPU usage to a loaded module. Additionally, if binary symbols are available and with call-stacks enabled for *Profile events*, it is possible to describe how a given function in a given module is invoked.

5.4.7 System Call Events

Windows core OS system calls are the interface into the Windows kernel which, from the developer point of view, consist of several APIs. This instrumentation serves the purpose of monitoring system calls made by user mode applications or kernel mode components. There are two types of *System Call events*: *Enter and Exit*. A *System Call Enter event* relates to an invocation of a system call and logs the address of the called system service routine. A *System Call Exit* event relates to an exit from a system call. *System Call events* are useful for statistical analysis on system call activities and latencies.

Chapter 6

IT Managment Platform Agent Profiling

6.1 Testbed

In the course of the research project we evaluated several operations management platforms in order to provide a central point of IT operations information and also a platform to deliver and aggregate security related information. The tested scenario builds on the scenario presented in Subsection 3.4.3 and was used for evaluating the agents of those platforms. The testbed scenario assumes a computer network where the machines are Windows 2008, Windows 2003, Windows XP and Windows Embedded arranged in a logical Windows domain.

Our focus is evaluating the impact of the platforms enforcing operational management on the systems. Of particular interest was the system behavior of the *Agent Processes and Threads* of the studied platforms.

We performed kernel trace analysis for the two platforms studied, and propose alternative solution for monitoring and managing such scenarios. We devised simple experiments that consist in measuring the impact of remote management and monitoring of the agents of the platforms. We tested several operational scenarios and provide some of most significant results next.

6.2 HP Operations Manager 8.10i Agent Scenario

The experiment started by deploying the agent on a Windows XP system and then analyzing the kernel event traces during monitoring and management operations specified by the operator.

In Figure 6.7 we can observe, in dark yellow, the Idle process, and, in other colors, the impact of HP Operations Manager *Agent processes* in the overall CPU usage of the system.

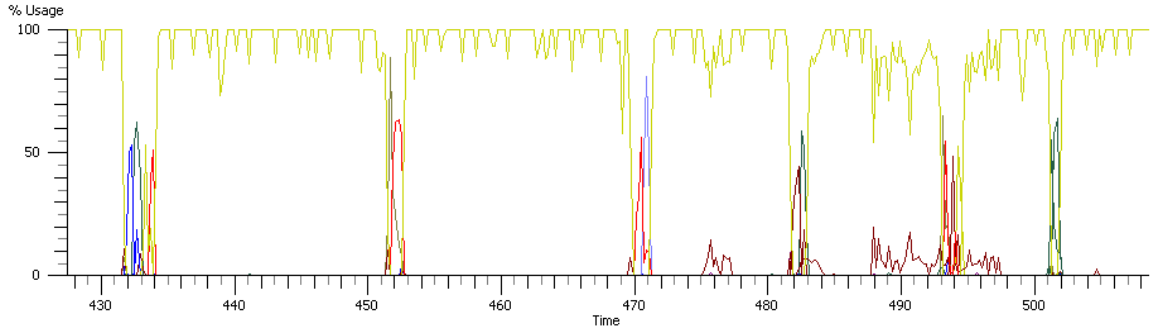

Figure 6.1: CPU Sampling of HP *Agent Processes* + Idle (System Overview)

In Figure 6.2 we can observe a detailed view of the impact of *Agent Processes* of HP Operations Manager 8.10i.

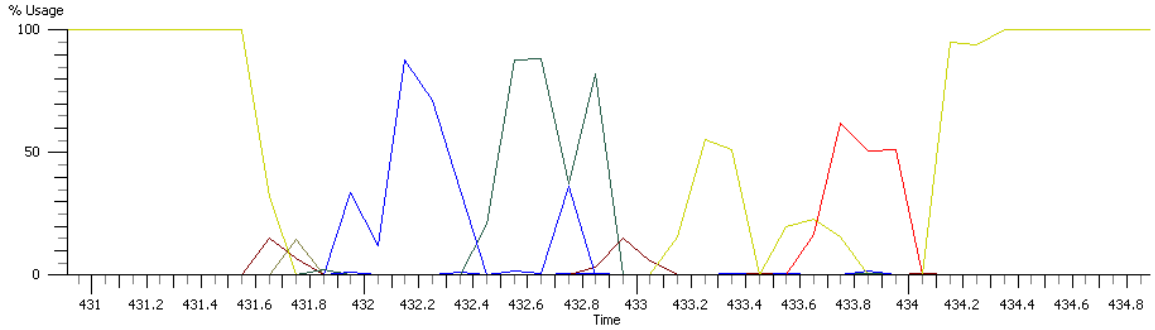

Figure 6.2: CPU Sampling of HP *Agent Processes* + Idle (Detailed View)

In Figure 6.3 we can observe the 100% utilization of the CPU upon executing monitoring and management operations, by the *Agent Processes*, on the HP Operations Manager 8.10i platform.

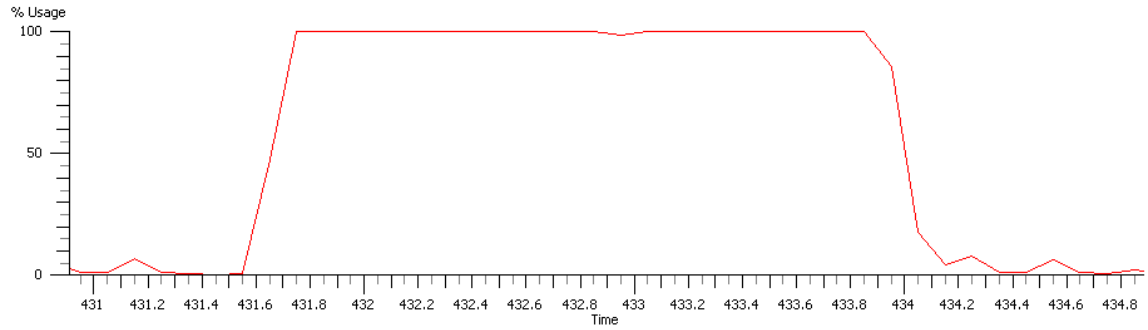

Figure 6.3: Total CPU Utilization (Detailed View)

These examples of the impact of *Agent Processes* on global system performance show that the HP Agents can have a significant impact in a critical control system. The scenarios consisted of simple monitoring and management operations. We could not restrict, by any known configuration, the system impact of the *Agent Processes* of HP Operations Manager 8.10i.

6.3 Microsoft Systems Center Operations Manager 2007 R2 Agent Scenario

The experiment started by deploying the agent on a Windows XP system and then analyzing the kernel event traces during monitoring and management operations specified by the operator.

In Figure 6.4 we can observe, in green, the Idle process, and the impact of Systems Center Operations Manager *Agent Processes* in the overall CPU usage of the system.

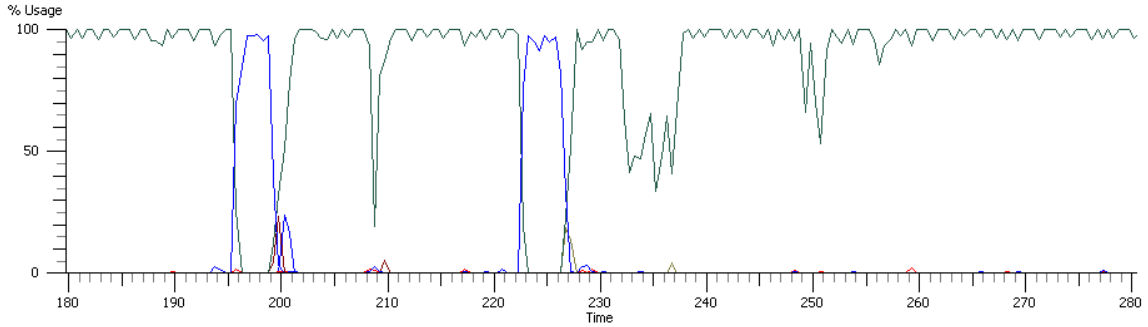

Figure 6.4: CPU Sampling of SCOM *Agent Processes* + Idle (System Overview)

In Figure 6.5 we can observe a detailed view of the impact of *Agent Processes* of Systems Center Operations Manager 2007 R2.

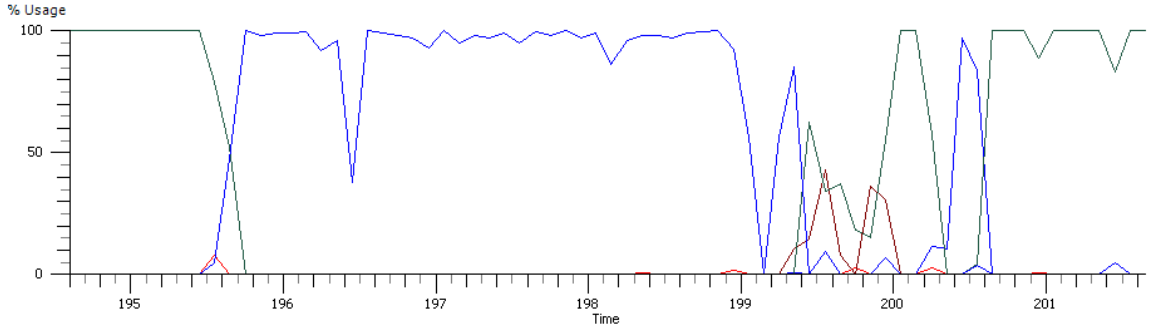

Figure 6.5: CPU Sampling of SCOM *Agent Processes* + Idle (Detailed View)

In Figure 6.6 we can observe the 100% utilization of the CPU upon executing monitoring and management operations, by the *Agent Processes*, on the Systems Center Operations Manager 2007 R2.

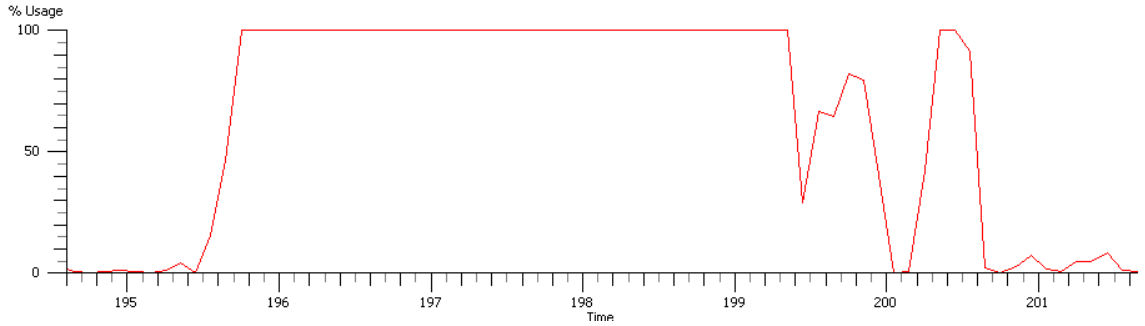

Figure 6.6: Total CPU Utilization (Detailed View)

These examples of the impact of *Agent Processes* on global system performance show that the Microsoft Systems Center Operations Manager 2007 R2 Agents can have a significant impact in a critical control system. The scenarios consisted of simple monitoring and management operations. We could not restrict, by any known configuration, the system impact of the *Agent Processes* Systems Center Operations Manager 2007 R2.

6.4 ETW Agent Scenario

We devised an experiment to evaluate ETW monitoring and profiling impact.

We created two Windows console applications: **rt-app**, a *event provider* which can generate on-demand ETW events; **rt-sup**, a *event consumer* which receives and handle real time events produced by **rt-app**. These are both user-mode applications, but these methods can be ported to a specific device driver. This is important since the task of monitoring control systems most certainly requires in-depth, driver level, instrumentation.

The test consisted of two concurrent ETW sessions, a kernel real-time tracing session and the application monitoring session, **rt-app** and **rt-sup**. The experiments took place on both a Windows 2008 Server Standard and on a Windows XP running in a VMWare virtual machine, so we can defend that these tests in physical machines would yield better results. The *event provider* application, **rt-app**, was instrumented in a way to generate, on demand, 20000 consecutive events with distinct payload. The *event consumer* application, **rt-sup**, links to the real-time session and writes the received events to a console application.

In Figure 6.7 we can observe, in green, the Idle process and the impact of **rt-sup** and **rt-app** in the overall CPU usage of the system.

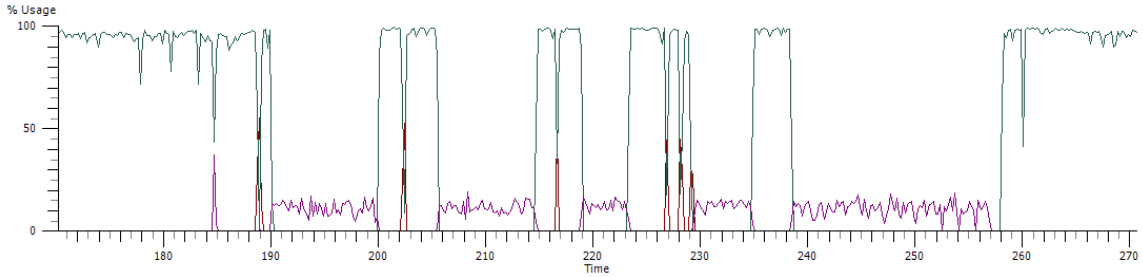

Figure 6.7: CPU Utilization of **rt-app** + **rt-sup** + Idle Process (Overview)

In Figure 6.8 we can observe a detailed view of the impact of **rt-app** and **rt-sup** in the overall system performance. Please note that the highest impact on the overall performance is not directly mapped to **rt-app** and **rt-sup**, the impact is due to user-mode and kernel-mode processes that handle IO operations of console applications.

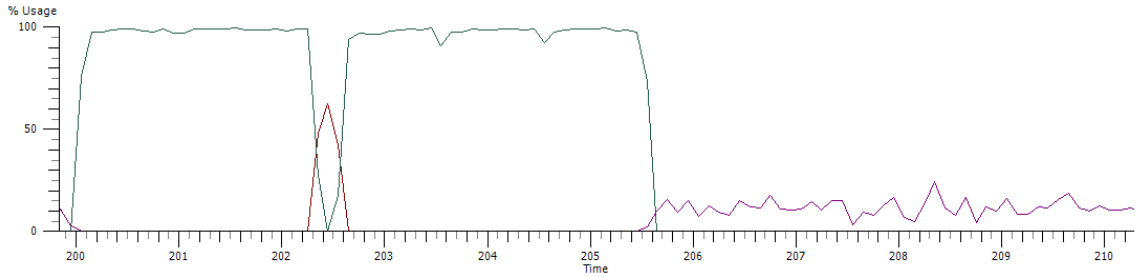

Figure 6.8: CPU Utilization of **rt-app** + **rt-sup** + Idle Process (Detailed View)

In Figure 6.9 we can observe the utilization of the CPU, under 100%, upon executing monitoring operations.

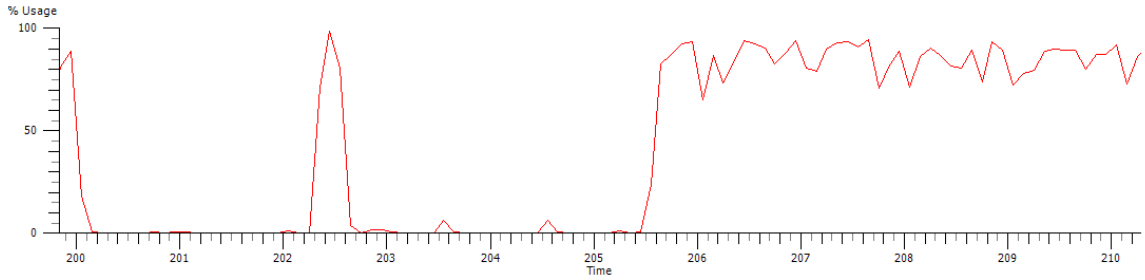

Figure 6.9: Total CPU Utilization (Detailed View)

6.5 Evaluation

The experiments described above are a small subset of the whole set of experiments we performed. Nevertheless, they graphically summarize our findings regarding the performance impact of the studied agents.

HP Operations Manager 8.10i agent is more than a simple service. The default installation of HP's agent deploys more than 15 individual packages on Windows XP, with several services supporting agent functionality.

Microsoft Systems Center Operations Manager 2007 R2 agent installs one service.

The management operations, that triggered agent execution, consisted in evaluating a small subset of system information (logged on users, running processes and few additional details). We have come to realize that the agents act has web servers parsing management and operations requests from the IT management platforms. The parsing and execution of commands bring higher performance overhead, that is due to the fact that these agents are generic by design.

To address the problems, stated above, we propose using fixed behavior monitoring agents. Fixed behavior monitoring agents require precise operational insight on the systems being monitored. That insight can be achieved by using ETW to profile these critical control systems in a pre-production environment and then constructing agents to supervise the behavior of the system and the control applications.

To further investigate our claims we created an experiment to observe the performance impact of using application event supervision, via ETW. The test application provided a shower of events with distinct payload and we could then verify causal order on the events received by the supervisor application. Additionally, we could attest the low performance impact of the monitoring techniques.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

In support of Defense in Depth strategy, defended along this research project for these critical utility IT infrastructures, we can argue that monitoring and proactively managing these infrastructures is of critical importance. The platforms offered by several vendors offer end-to-end monitoring and root cause analysis, but that comes with a significant cost that is certainly unmanageable in a critical control system scenario.

We have studied, to some extent, the impact of monitoring and management agents of these platforms. Additionally, we investigated techniques to develop low-impact monitoring solutions. We have shown that applications instrumented with ETW can benefit from precise light-weight correlation of application and OS activities. Likewise, management tools can be developed to take advantage of the core system events and ETW analysis techniques. Creating better monitoring and management agents will benefit IT operations on such infrastructures.

The importance of the studied questions grows when we consider that in the near future the number of critical control systems based on COTS will continue to grow.

7.2 Future Work

One interesting research followup would be investigating diversity capabilities of COTS systems supporting critical utility IT infrastructures. Our work focused on Microsoft Windows OS but the critical control systems implemented on Linux systems have the same constraints as the Windows OSs we investigated.

In Windows based control systems incorporating ETW monitoring into applications would allow to achieve end-to-end monitoring. Evaluating the end-to-end impact of a monitoring solution in critical utility IT infrastructures would yield insight into scalability and performance problems, and even global application level abnormal behavior detection. Additionally, the development of a light-weight multipurpose agent bearing kernel-level application monitoring and system-wide management capabilities. Such agent could be implemented in order to provide SNMP functionality, given its inherent low overhead capabilities.

Studying the possibility of creating state-machine supervisors to the control systems applications became more interesting as we discovered the capabilities of ETW mechanisms. A future direction on our research could be the feasibility of such systems.

Integrating the knowledge provided by the studied monitoring capabilities into Network and System Intrusion Detection Systems (IDS) would extended the common capabilities of such systems, the extent of the improvement should be subject to further study. Similarly, together with Security Information and Event Management (SIEM) platforms the potential to achieve global coverage on the security of critical utility IT infrastructures.

Bibliography

[1] A. Daneels and W. Salter. What is SCADA? In *Proc. of Int. Conf. on Accelerator and Large Experimental Physics Control Systems*, pages 39–343, 1999. 1.1

[2] P.P. Purpura. *Terrorism and homeland security: an introduction with applications*. Butterworth-Heinemann, 2007. 1.1

[3] European Commission. SmartGrids - Towards Smart Power Networks, 2005. URL `http://www.smartgrids.eu/`. 1.1

[4] M.A. Winniford, S. Conger, and L. Erickson-Harris. Confusion in the Ranks: IT Service Management Practice and Terminology. *Information Systems Management*, 26(2):153–163, 2009. 2.1

[5] Office of Government Commerce (OGC). ITIL - Information Technology Infrastructure Library. URL `http://www.itil-officialsite.com/home/home.asp`. 2.1

[6] ISACA - Control Objectives for Information and related Technology, Oct. 2009. URL `http://isaca.org/cobit/`. 2.1, 2.1.3

[7] M. Damianides. Sarbanes–Oxley and IT Governance: New guidance on IT control and compliance. *EDPACS*, 31(10):1–14, 2004. 2.1.2

[8] Internation Organization for Standardization. ISO/IEC 20000 Information technology - Service management - Part 1: Specification. URL `http://www.iso.org/iso/catalogue_detail?csnumber=41332`. 2.1.4

[9] J. Woodward. Information assurance through defense in depth. Technical report, Command, Control, Communications and Computer System; U.S. Department of Defense, 2000. 2.5

[10] CRUTIAL - CRitical UTility InfrastructurAL Resilience, 2005 - 2008. URL http://crutial.cesiricerca.it/. 2.6

[11] P. Verissimo, N. Ferreira Neves, and M. Correia. The CRUTIAL reference critical information infrastructure architecture: a blueprint. *International Journal of System of Systems Engineering*, 1(1):78–95, 2008. 2.6

[12] D. Harrington, R. Presuhn, and B. Wijnen. An architecture for describing simple network management protocol (SNMP) management frameworks. *Request for Comments*, 3411, 2002. 2.7, 3.4.3

[13] DMTF Web Services for Management, Oct. 2009. URL http://www.dmtf.org/standards/wsman/. 2.7, 3.4.2.3, 3.4.3

[14] P. Verissimo and L. Rodrigues. *Distributed systems for system architects*. Kluwer Academic Publishers, 2001. 2.8

[15] BMC's portfolio of Business Service Management Solutions, Oct. 2009. URL http://www.bmc.com/solutions. 3.3.1

[16] BMC Atrium Change Management Database, Oct. 2009. URL http://www.bmc.com/products/offering/bmc-atrium-cmdb.html. 3.3.1

[17] BMC Atrium CMDB Enterprise Manager, Oct. 2009. URL http://www.bmc.com/products/product-listing/53556216-141391-2117.html. 3.3.1

[18] BMC Atrium Orchestrator, Oct. 2009. URL http://www.bmc.com/products/product-listing/90902406-157022-1134.html. 3.3.1

[19] BMC Dashboards for BSM, Oct. 2009. URL http://www.bmc.com/products/product-listing/69130935-140704-1230.html. 3.3.1

[20] BMC Analytics for BSM, Oct. 2009. URL http://www.bmc.com/products/product-listing/77980717-153648-2455.html. 3.3.1

[21] CA Infrastructure Management Solutions, Oct. 2009. URL http://www.ca.com/us/infrastructure-management.aspx. 3.3.2

[22] CA Network and Systems Management, Oct. 2009. URL http://www.ca.com/us/system-management.aspx. 3.3.2

[23] CA Spectrum Automation Manager, Oct. 2009. URL http://www.ca.com/us/server-provisioning.aspx. 3.3.2

[24] EMC IT Management solutions, Oct. 2009. URL http://www.emc.com/products/category/it-management.htm. 3.3.3

[25] EMC IT Operations Intelligence Solutions, Oct. 2009. URL http://www.emc.com/products/family/smarts-family.htm?context=it-operations-insight. 3.3.3

[26] HP Business Optimization Technologies, Oct. 2009. URL https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-10_4000_100__. 3.3.4

[27] HP Operations Manager 8.10i for Windows, Oct. 2009. URL https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-28^37673_4000_100__. 3.3.4

[28] HP Operations Smart Plug-ins (SPIs), Oct. 2009. URL https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-28^41718_4000_100__. 3.3.4

[29] HP Performance Manager , Oct. 2009. URL https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-28^1792_4000_100__. 3.3.4

[30] HP Reporter, Oct. 2009. URL https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-28^1734_4000_100__. 3.3.4

[31] Hp sitescope, Oct. 2009. URL https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-25^849_4000_100__. 3.3.4

[32] HP Change Management Database, Oct. 2009. URL https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-15-25^1059_4000_100__. 3.3.4

[33] IBM Tivoli Availability Process Manager, Oct. 2009. URL http://www-01.ibm.com/software/tivoli/products/availability-process-mgr/. 3.3.5

[34] IBM Tivoli Monitoring, Oct. 2009. URL http://www-01.ibm.com/software/tivoli/products/monitor/. 3.3.5

[35] IBM Tivoli Performance Analyzer, Oct. 2009. URL http://www-01.ibm.com/software/tivoli/products/performance-analyzer/. 3.3.5

[36] IBM Tivoli Configuration Manager, Oct. 2009. URL http://www-01.ibm.com/software/tivoli/products/config-mgr/. 3.3.5

[37] IBM Tivoli Data Warehouse, Oct. 2009. URL http://www-01.ibm.com/software/tivoli/products/data-warehouse/. 3.3.5

[38] Microsoft Systems Center Solutions, Oct. 2009. URL http://www.microsoft.com/systemcenter/products/default.mspx. 3.3.6

[39] Microsoft Systems Center Configuration Manager 2007, Oct. 2009. URL http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx. 3.3.6

[40] Microsoft Systems Operations Manager 2007 R2, Oct. 2009. URL http://www.microsoft.com/systemcenter/operationsmanager/en/us/default.aspx. 3.3.6

[41] DMTF Common Information Model (CIM) Standards, Oct. 2009. URL http://www.dmtf.org/standards/cim. 4.2

[42] Distributed Management Task Force, Oct. 2009. URL http://www.dmtf.org. 4.2

[43] Microsoft Windows SDK. URL http://msdn.microsoft.com/en-us/windowsserver/bb980924.aspx. 5.2

[44] Microsoft Windows Performance Analysis Tools, Oct. 2009. URL http://msdn.microsoft.com/en-us/performance/cc825801.aspx. 5.2

[45] Microsoft Performance Xperf Tools, Oct. 2009. URL http://msdn.microsoft.com/en-us/library/cc305221.aspx. 5.2