Rittal – The System.

Faster – better – everywhere.

Whitepaper –
Security management for data centre infrastructures

Bernd Hanstein

Contents

Author: Bernd Hanstein

After receiving a Diplom degree in physics from the Justus Liebig University in Gießen in 1987, Bernd Hanstein joined the central research unit of Siemens AG, where he worked on test methods for highly integrated circuitry. He subsequently occupied various positions within the Public Networks Group of Siemens AG, with responsibility for the implementation of major ICT projects. In 2002, Bernd Hanstein moved to Siemens VDO Automotive as senior manager responsible for the worldwide system testing of in-vehicle multimedia devices. Since 2007, he has been head of IT product management at Rittal in Herborn. His key interests: IT components, RiMatrix system solutions and data centre technologies.

List of figures

List of tables

Executive summary

Data centres are essential communication components in a networked, digital world. They are needed to provide data and services and can therefore be found in every walk of life. Data centres also represent a key data processing and communication hub within critical supply infrastructures. Consequently, any failure has serious consequences for the general public.

In its report on Germany's IT security situation in 2015 [Ref. 1], the BSI (German Federal Office for Information Security) cites some current examples in underlining the threats and potential risks. These include an increase in cyber attacks, which are also aimed at government agencies and target critical infrastructures. The BSI has published an entire catalogue of measures addressing basic IT security [Ref. 2]. Similar steps have been taken internationally, for example by the Department of Homeland Security in the United States [Ref. 3].

The German government's legislation to improve the security of IT systems [Ref. 4] addresses the need to ensure special protection for critical infrastructures and sets out obligations for operators and manufacturers alike.

These issues are not solely of interest to large companies and the operators of critical infrastructures, though. With the Internet of Things and Industry 4.0 pushing Internet technology all the way to the machinery on the production line [Ref. 5], they are also becoming increasingly important for small and mid-size companies.

In this connection, the BSI has formulated recommendations [Ref. 6] for checking critical software so as to detect and rectify weak points. In the case of data centres, this makes data centre infrastructure management (DCIM) software particularly important given that it monitors and controls all components of the physical infrastructure.

- The DCIM software and all active components must be hardened.
- Stringent assignment and documentation of roles and rights is a must.
- The use of DCIM software enables data centres to be monitored and controlled transparently.
- Incidents can be linked, reporting chains generated and workflows agreed for an automated response to threats and faults.

This white paper therefore sheds light on two aspects of a data centre's management software:

- How secure is DCIM software itself in conjunction with all the active components of a physical data centre infrastructure?

and

- How can DCIM software boost security in the data centre environment?

Risk vectors in the physical data centre infrastructure

As the backbone of an increasingly digital society, data centres house a large number of servers, storage systems and active network components (switches, routers). To ensure the smooth operation of these active IT components, an appropriate physical IT infrastructure is required to provide a reliable power supply and power backup along with climate control geared to the relevant requirements. The data centre and all its components must also be protected against traditional potential threats such as:

- Fire
- Smoke
- Water / steam
- Dust
- Falling debris
- Vandalism
- Break-ins
- EMC (irradiation, radiation)

The necessary protective measures are provided by a whole host of products and solutions based on international norms and standards as described in a separate white paper on physical security in IT and data centre technology [Ref. 7].

Continuous, reliable monitoring of a data centre's operating parameters is equally important, because faults in the physical IT infrastructure can also impair operation and thus affect service level agreements (SLAs) with customers. Such faults in the operating parameters may include the following:

- Power failure of the energy supplier
- Faults on supply lines
- Faults in the current distribution path (main infeed, sub-distributor, socket systems)
- Climate control failure (generation, transportation and distribution of cooling energy)
- Failure of individual sensors and the monitor system (excessive temperatures, moisture, leaks, etc.)

The large number of components in a physical IT infrastructure and the numerous operating parameters to be monitored make automated monitoring and evaluation of data a must.

This task is performed by the DCIM software [Ref. 9], as it monitors and controls a data centre's entire physical IT infrastructure. This includes, for example:

- Power supply and reliability
- Generation and distribution of cooling energy
- Environmental parameters (temperature, humidity, etc.)

- Capacity management (weight, height units and cooling)
- Security in the data centre
- Efficiency and energy consumption

The individual parameters can be displayed in user-specific views on a hierarchical dashboard (Figure 1).

Figure 1: DCIM software dashboard

Workflows can link individual incidents, which enables alarm scenarios to be defined and responses – including automated ones – to be initiated. Appropriate interfaces can forward the necessary information and alarms to higher-level management systems.

Security aspects of DCIM software

Every monitoring system and every DCIM solution is made up of several components, as can be seen from the following list and the DCIM architecture shown in Figure 2:

- Application software
- Database system
- Operating system (virtualised if necessary)
- Physical server

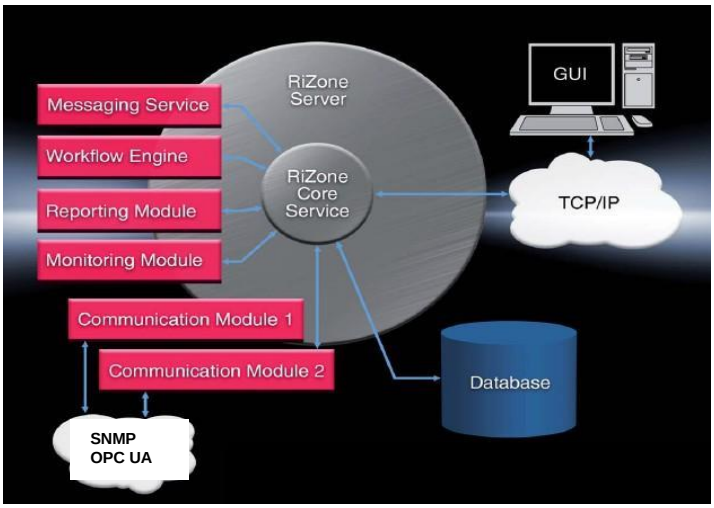


Figure 2: DCIM architecture

This shows that a DCIM solution, like any other IT system, can be subject to cyber attacks. Data centres and thus their monitoring systems often form part of a critical infrastructure. The BSI's report [Ref. 1], which is published on an annual basis, reveals that the number of threats is growing.

Threat	2014	2015
Cloud computing		→
Software vulnerabilities	→	↑
Hardware vulnerabilities		→
User behaviour and manufacturer responsibility		↑
Cryptography		→
Internet protocols		↑
Mobile communication		↑
App security		↑
Industrial control system security		↑
Malware	↑	↑
Social engineering	↑	→
Targeted attacks – APT	→	↑
Spam	↑	↑
Botnets	→	↑
Distributed denial of service (DDoS) attacks	→	→
Drive-by exploits and exploit kits	→	↑
Identity theft	↑	↑

Key
Level of threat in 2015 (low, average, high) ↓ → ↑

Table **1** below provides an overview of activities.

Threat	2014	2015
Cloud computing		→
Software vulnerabilities	→	↑
Hardware vulnerabilities		→
User behaviour and manufacturer responsibility		↑
Cryptography		→
Internet protocols		↑
Mobile communication		↑
App security		↑
Industrial control system security		↑
Malware	↑	↑
Social engineering	↑	→
Targeted attacks – APT	→	↑
Spam	↑	↑
Botnets	→	↑
Distributed denial of service (DDoS) attacks	→	→
Drive-by exploits and exploit kits	→	↑
Identity theft	↑	↑

Key
Level of threat in 2015 (low, average, high) ↓ → ↑

Table 1: Potential risks (BSI 2015)

Operators and manufacturers alike must take appropriate measures for critical infrastructures in particular, as also stipulated by German legislation on IT security [Ref. 4]. In this connection, the BSI has also published a recommendation for checking software solutions [Ref. 6]. Similar recommendations have been made by the Department of Homeland Security in the United States [Ref. 3]. Carnegie Mellon University's Software Engineering Institute [Ref. 8] has published an overview of possible weak points.

The following sections therefore provide a detailed description of checking the DCIM solution. It is vital to analyse not only the DCIM system, but also all active components of the physical IT infrastructure.

It is inadequate to protect the data centre infrastructure with a firewall. The combination of protective measures must be comprehensively optimised to ensure reliable protection.

DCIM weak point analysis

The result of a weak point analysis of the RiZone DCIM software depends on how the Windows server is configured. The operating instructions [Ref. 9] indicate the ports required for operation:

- 161 (SNMP get/set)
- 162 (SNMP trap handler)
- 800 (certificate provider)
- 3389 (RDP)

- 4433 (https for roles and rights)
- 22222 & 22223 (RiZone core service port)

In principle, the remaining ports can be sealed so as not to offer any possibility of attack.

The RiZone DCIM software was tested using Greenbone/OpenVAS [Ref. 9] with the Windows Server 2008r2 and Windows Server 2012r2 operating systems.

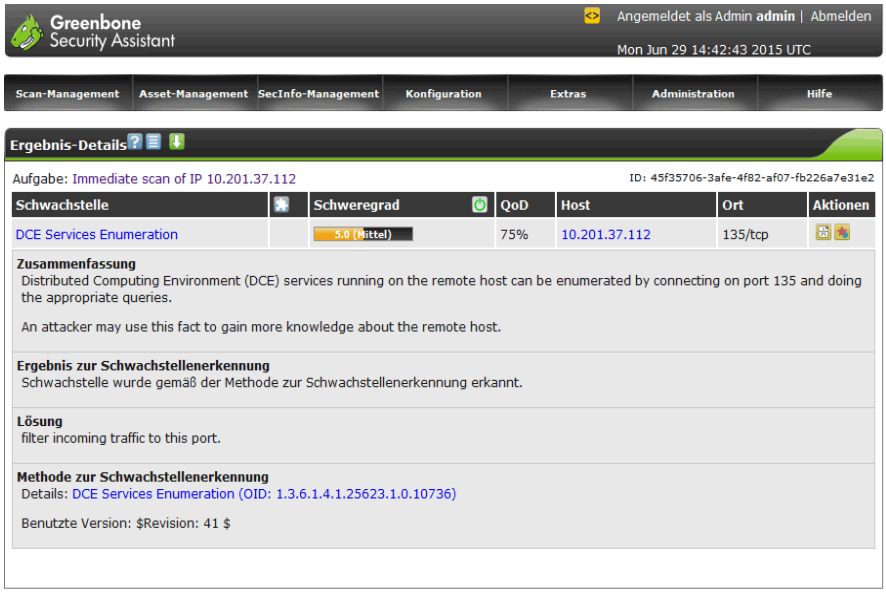


Figure 3: OpenVAS report

OpenVAS [Ref. 9] is a tool that enables a comprehensive analysis for possible weak points in an IP-based system as in the case of a DCIM/monitoring system for the IT infrastructure. Different depths of testing can be defined so as to facilitate the identification and location of potential weak points. The tool's central component is an NVT (network vulnerability test) scanner that is supplied with current patterns and searches the network for potential weak points. The weak points detected can then be categorised and prioritised so that corrective actions can be defined and implemented.

Risks were detected when checking Rittal's RiZone DCIM software with the help of OpenVAS as shown in Figure 3. These danger areas can be traced back to the operating system and can be completely eliminated with the help of the Windows firewall.

Checking active IT infrastructure components

A typical data centre (Figure 4) contains a multitude of active IT infrastructure components that have IP interfaces and are incorporated into the network. The potential threats applying to these components are the same as the ones described above for the DCIM software.

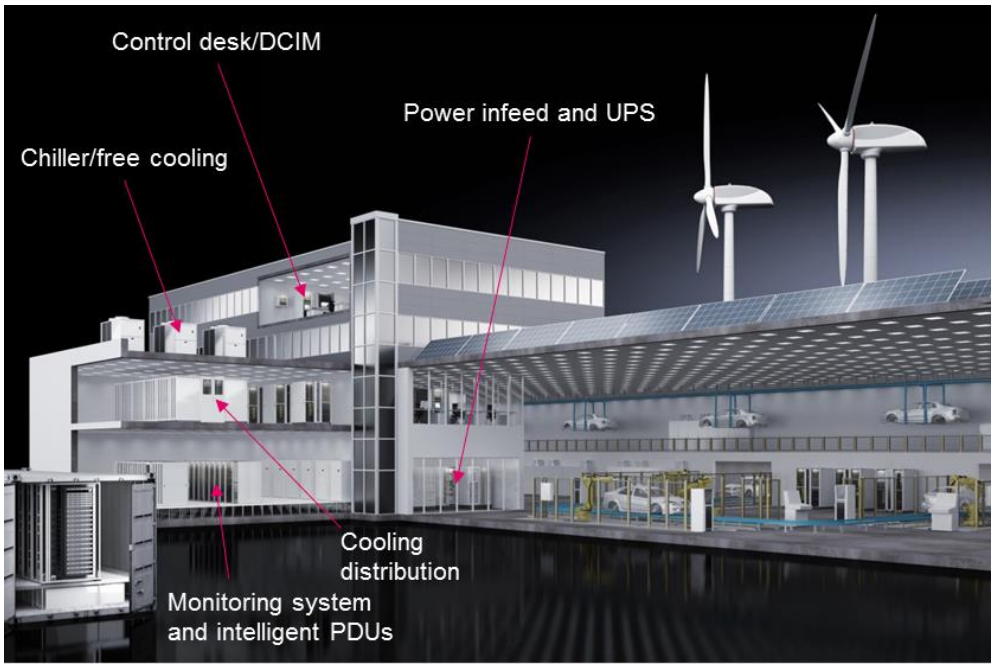


Figure 4: Active IT infrastructure components

The following sample test of the CMC monitoring system (Figure 5) was performed using tenable network security's Nessus V.6.4.1 software [Ref. 11].

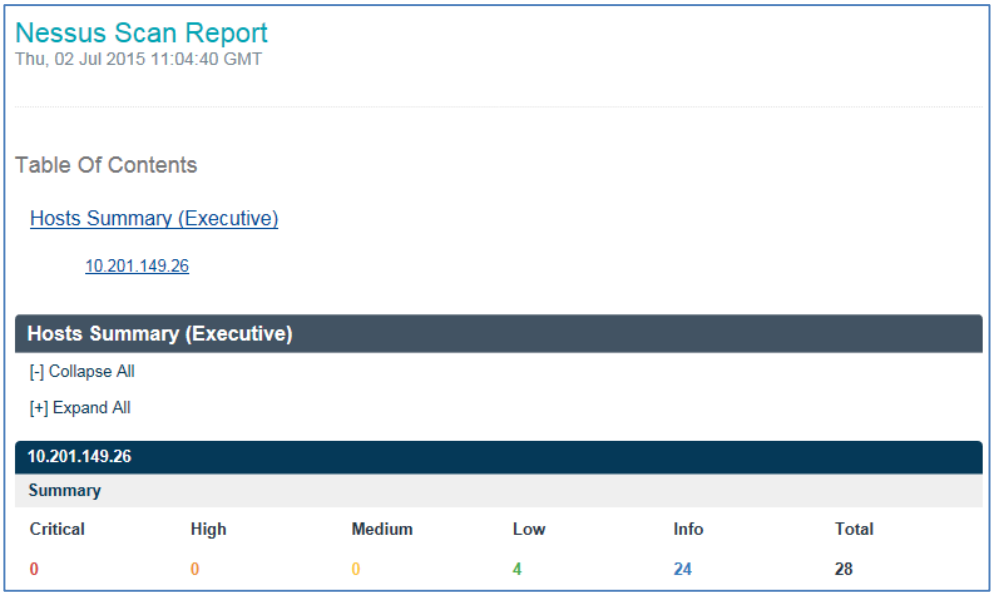
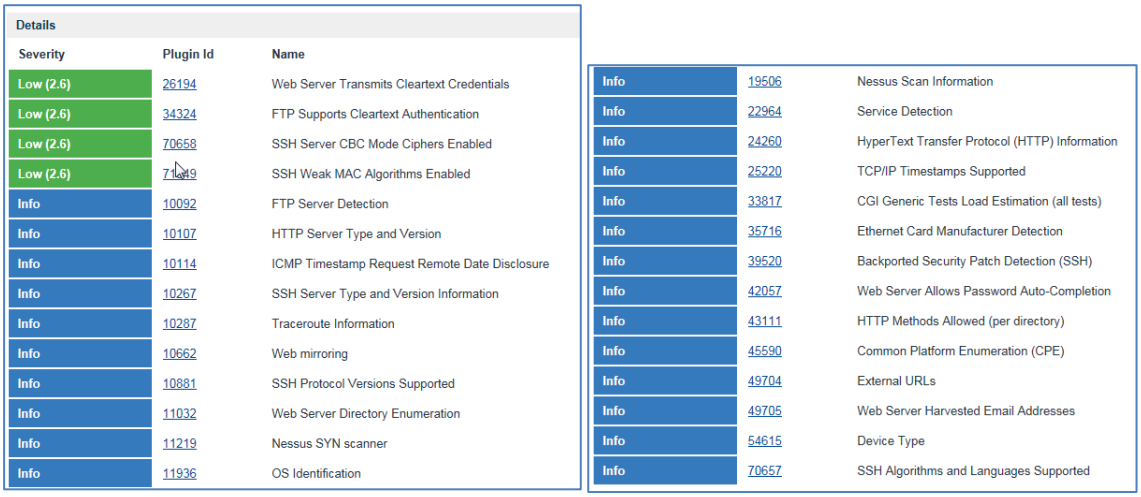


Figure 5: Nessus report on Rittal's CMC monitoring system

Nessus [Ref. 11] is a web-based NVT scanner for identifying weak points. It consists of an HTTP server and a web client. The LDAP protocol is supported, which allows the Nessus server to be authenticated in the network.

Tests can be performed on IPv4 and/or IPv6 addresses (CIDR annotation for more efficient use of the address space). The results of an analysis can be exported or displayed on a dashboard (see e.g. Figure 5).

Nessus scans the network components, applications, databases and operating systems for vulnerability, identifying weak points and security gaps. The result of the scan indicates weak points and corrective action so as to enable the relevant interfaces to be made secure or ensure an appropriate measure is carried out in the data centre's customer network (see e.g. Figure 6).



Details

Severity	Plugin Id	Name
Low (2.6)	26194	Web Server Transmits Cleartext Credentials
Low (2.6)	34324	FTP Supports Cleartext Authentication
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10662	Web mirroring
Info	10881	SSH Protocol Versions Supported
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	33817	CGI Generic Tests Load Estimation (all tests)
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	49704	External URLs
Info	49705	Web Server Harvested Email Addresses
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported

Figure 6: Detailed Nessus report

The same tests/hardening measures must be performed for all active components in the physical infrastructure.

DCIM – an essential component of data centre security

Roles and rights

A DCIM solution is a powerful tool that helps not only monitor but also control the physical IT infrastructure. For example, a socket system's individual sockets can be switched remotely or a chiller's operating parameters can be modified. Only authorised specialist personnel are permitted to perform such operations in the IT infrastructure. Stringent application of roles and access rights in the DCIM/monitoring system is therefore vital:

- Monitor
- Evaluate
- Modify

- Administrative rights

Roles and responsibilities must be documented as appropriate in the data centre's operating and emergency manual. Proof of these measures must be provided in the event of an audit.

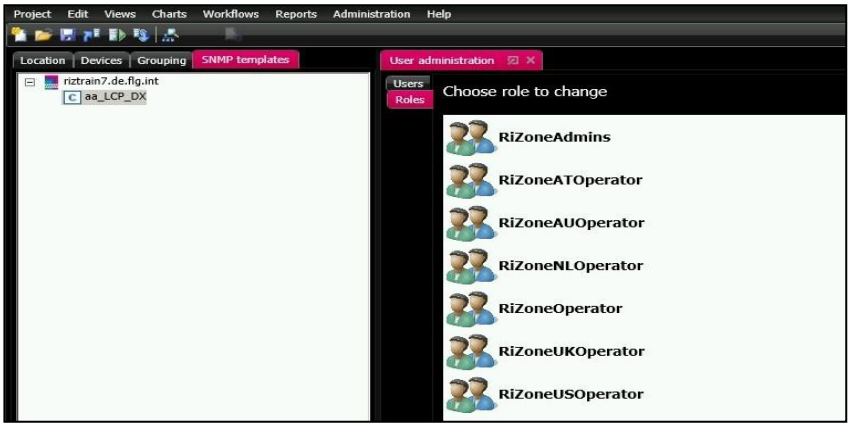


Figure 7: Assigning roles and rights in the DCIM tool

Displaying results

The DCIM system is able to record all incidents and the relevant operating parameters and file these in a (SQL) database. It is vital to assign the active components to the data centre topology (location in enclosure, bayed enclosure suite, room, floor, building, town/city, country) so that a direct reference between an incident and the position of the relevant component can be generated in a hierarchical display.

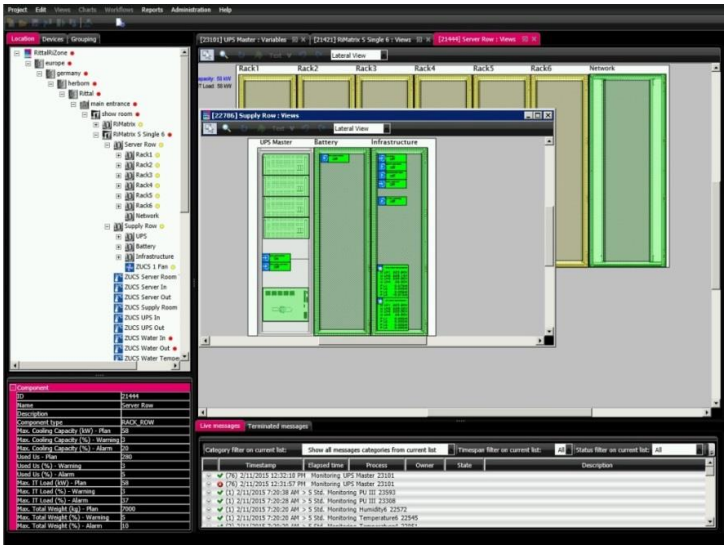


Figure 8: Online monitoring in the DCIM tool

The previously agreed roles and rights make it possible to define specific views that can be assigned to the relevant user circle.

Monitoring and trend analysis

All values imported or calculated can be grouped and shown in diagrams as required and compared with historical values from the (SQL) database. The DCIM system helps calculate formulas that enable the measured values to be linked and calculations to be performed, for example to calculate the PUE.

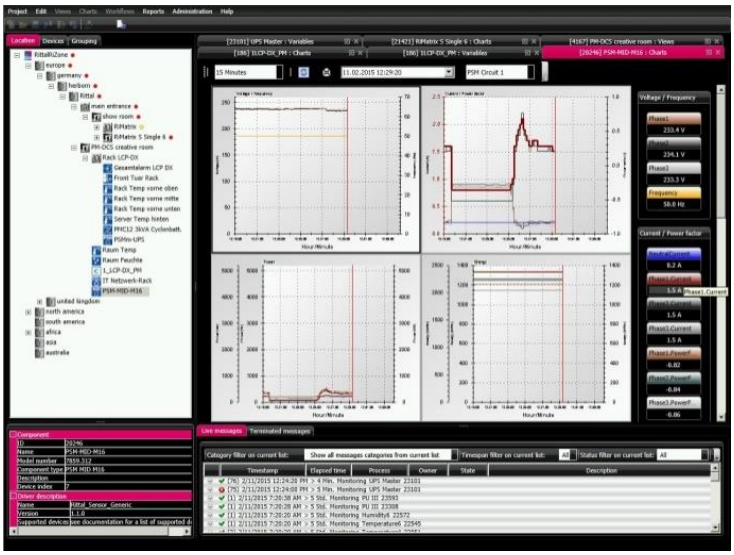


Figure 9: Trend analyses in the DCIM tool

This can be used as a basis for generating reports in an automated process, for example to document the change in electricity costs. These functions can be geared to the relevant user groups based on the roles and rights.

Alarm management & workflows

The DCIM software's workflow engine depicts automated monitoring and control scenarios based on the previously defined threshold values for warnings and alarms.

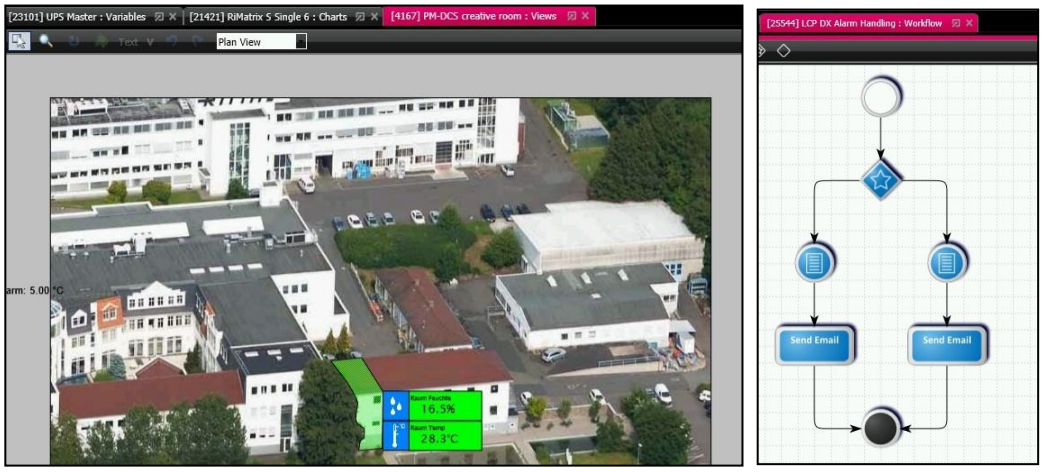


Figure 10: Workflows and alarm scenarios in the DCIM tool

The option of linking incidents gives users a view of the data centre that is not possible with an isolated consideration of the individual components. Alarms overlay schematic or photographic representations. The complete overview is customised for each application.

Messages (warnings, alarms) can also be dealt with on a targeted basis. The history documents who dealt with which incident and when.

Integration into management systems

The possibility of forwarding data from the DCIM software to a management tool for the server, operating system, visualisation and application (Figure 11) allows data centre operators to create a standardised dashboard.

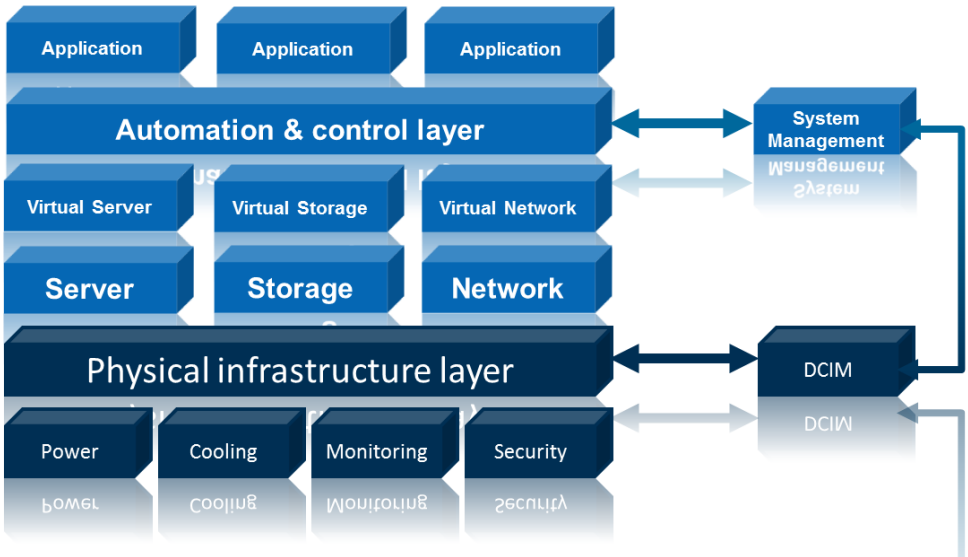


Figure 11: Interplay in the virtualisation context

SNMP and OPC UA protocols are supported, which also enables incorporation into a BCS/BMS.

References

Ref. 1 BSI (German Federal Office for Information Security), The State of IT Security in Germany 2015, link: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf

Ref. 2 BSI (German Federal Office for Information Security), IT Grundschutz, link: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

Ref. 3 Department of Homeland Security, Critical Infrastructure Vulnerability Assessment, link: http://www.dhs.gov/critical-infrastructure-vulnerability-assessments

Ref. 4 Federal Law Gazette 2015 Part I No. 31, published in Bonn on 24 July 2015, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), link: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__//*[@attr_id='bgbl115s1324.pdf']__1440083508634

Ref. 5 BMBF (Federal Ministry of Education and Research), Industry 4.0 platform, "The background to Plattform Industrie 4.0"; link: http://www.plattform-i40.de/I40/Navigation/EN/ThePlatform/PlattformIndustrie40/plattform-industrie-40.html

Ref. 6 BSI (German Federal Office for Information Security), Open Vulnerability Assessment System (OpenVAS), link: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Tools/OpenVAS/OpenVAS.html

Ref. 7 Rittal white paper: Physical security in IT and data centre technology

Ref. 8 Overview of possible weak points: Vulnerability Notes Database, Carnegie Mellon University, Software Engineering Institute, link: https://www.kb.cert.org/vuls/

Ref. 9 Rittal RiZone operating manual, link: http://www.rittal.de/downloads/rimatrix5/software/V3_6/Manual_Rizone_Appendix36_V10_en.pdf

Ref. 10 OpenVAS, link: http://www.openvas.org/index.html

Ref. 11 tenable network security, link: http://www.tenable.com/products/nessus-vulnerability-scanner

Ref. 12 Naming convention for weak points in IT systems, link: https://cve.mitre.org/cve/cna.html

List of abbreviations

APT	Advanced persistent threat (targeted attack on critical IT infrastructures)
BCS	Building control system
BMS	Building management system
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CBC	Cipher Block Chaining Mode (encryption of a clear text block)
CIDR	Classless Inter-Domain Routing
CMC	Computer Multi Control (basic monitoring system unit)
CPE	Common Platform Enumeration (standardised naming convention for designating weak points in IT systems)
CVE	Common Vulnerabilities and Exposures (standardised naming convention for security gaps in IT systems)
DC	Data centre
DCE	Distributed Computing Environment
DCIM	Data Centre Infrastructure Management
DDoS	Distributed Denial of Service
DoS	Denial of Service (failure of a service due to overloading of resources)
EMC	Electromagnetic compatibility
FTP	File Transfer Protocol
GUI	Graphical user interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol (protocol for exchanging information and error messages)
IoT	Internet of Things
IPv4	Internet Protocol Version 4 (using 32-bit addresses)
IPv6	Internet Protocol Version 6 (using 128-bit addresses)
IT	Information technology
LDAP	Lightweight Directory Access Protocol (directory service for authorisation)
NVT	Network Vulnerability Test
OLE	Object Linking and Embedding
OPC UA	Open Platform Communications Unified Architecture
OS	Operating system
PUE	Power usage effectiveness

RDP	Remote Desktop Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell (encrypted network protocol)
SSL	Secure Sockets Layer (encryption protocol for data transfer)
SW	Software
SYN	SYN flood (denial of service attacks) on an incomplete TCP connection
TCP/IP	Transmission Control Protocol / Internet Protocol
U	Height unit
URL	Uniform Resource Locator (IT resource and associated access method)
VAS	Vulnerability Assessment System

Rittal – The System.

Faster – better – everywhere.

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

RITTAL GmbH & Co. KG
Auf dem Stützelberg · 35726 Herborn · Germany
Phone + 49 (0)2772 505-0 · Fax + 49 (0)2772 505-2319
E-mail: info@rittal.de · www.rittal.com · www.rimatrix5.de