REVISITING CERN SAFETY SYSTEM MONITORING (SSM)

T. Hakulinen, P. Ninin, R. Nunes, T. Riesco-Hernandez, CERN, Geneva, Switzerland

Abstract

CERN Safety System Monitoring (SSM) is a system for monitoring state-of-health of the various access and personnel safety systems at CERN since more than three years. SSM implements monitoring of different operating systems, network equipment, storage, and special devices like PLCs, front ends, etc. It is based on the monitoring framework Zabbix, which supports alert notifications, issue escalation, reporting, distributed management, and automatic scalability. The emphasis of SSM is on the needs of maintenance and system operation, where timely and reliable feedback directly from the systems themselves is important to quickly pinpoint immediate or creeping problems. A new application of SSM is to anticipate availability problems through predictive trending that allows one to visualize and manage upcoming operational issues and infrastructure requirements. Work is underway to extend the scope of SSM to all access and safety systems managed by the access and safety team with upgrades to the monitoring methodology as well as to the visualization of results.

INTRODUCTION

Safety System Monitoring (SSM) [1] is a framework for monitoring the computing infrastructure of CERN safety-related systems, such as the access and safety systems of LHC, SPS, and PS. The goal of SSM is to easily monitor these highly heterogeneous systems, and to present the access and safety maintenance teams an accurate overall picture of the functioning of the various parts of the monitored systems. While the monitoring system is primarily aimed at the maintenance teams, some elements are still available to access operators and safety personnel.

After some years of experience with the original implementation of SSM, improvements were due: A new version of the monitoring tool offers easy application of visualization and trending as well as better overall performance. Any new features are being implemented on a new SSM instance while old systems, still monitored on the old instance, are being migrated to the new one, the two coexisting during an interim period.

MONITORED SYSTEMS

The following access and safety systems are the target of SSM:

- **LACS** (LHC Access Control System) – who enters the LHC and when.
- **LASS** (LHC Access Safety System) – is it safe for beam or access.
- **PACS** (PS Access Control System) – who enters the PS complex and when.
- **PASS** (PS Access Safety System) – is it safe for beam or access.
- **SPS PSS** – integrated personnel safety system for the SPS complex.
- **SUSI** (Surveillance des Sites) – who enters CERN sites and areas other than the accelerators.
- **CSAM** (CERN Safety Alarm Monitoring) – alarms for the fire brigade.
- **Sniffer** – gas detection and alarm.
- **SIP** (Site Information Panels) – display relevant info at access points.
- **SSA** (Safety System Atlas) – Access and personnel safety system for the ATLAS detector.

CERN access and safety systems typically consist of many different kinds of devices, such as Windows and Linux servers, operator posts, panel-PCs, PLCs, video cameras, interphones, card readers, biometry scanners, etc. These devices come from many different vendors, and they are nowadays mostly directly network connected. Access systems reside mainly in the CERN Technical Network (TN) but some devices reside also in the General Purpose Network (GPN). The most important systems (some of the safety systems) have their own private networks.

It is to manage this complexity in a unified manner that the SSM system was conceived: The goal was to build an integrated system for monitoring all safety and access systems managed by the CERN access and safety teams in a coherent and reliable manner. SSM is based on a freely available monitoring system Zabbix [2]. The main reasons for that choice are the openness and easy configurability of Zabbix, its out-of-the-box support for both Windows and Linux/Unix systems, SNMP and IPMI support, Oracle support, it being free of charge, and the fact that the access and safety teams have experience on it since some time.

DESIGN PRINCIPLES

The general design of the SSM system is based on the following basic principles:

- **Clarity**: Aim to apply a no-nonsense approach to system monitoring to offer the clearest possible picture of the state of the various systems to the maintenance and operation teams. In practice, use global status displays with simple traffic-light-style graphics, from which it is possible to dive deeper into the details if necessary.
- **Simplicity**: Use well-defined interfaces with clear functional separation. Use existing systems and CERN standard services whenever possible.
- **Reliability**: Put in place self-diagnostic checks to tell if the displayed information is trustworthy.

ISBN 978-3-95450-139-7

- **Independence**: Look at the system to be monitored from the outside and avoid using information produced by that system. Go to the source whenever possible (example: access PLCs directly).
- **Maintainability**: Keep scripts and database structure simple and easy to understand with up to date documentation.
- **Accessibility**: Must work with all major web-browsers and handheld devices from anywhere.
- **Confidentiality**: Access is to be limited to a well-defined group and a login with CERN password required.

SSM ARCHITECTURE CHANGES

The architecture of the original SSM is presented in detail in [1] so here are only listed changes to that architecture:

- A new version of Zabbix, 2.0.8 is being used as the monitoring engine.
- A master Zabbix server is connected to a local MySQL database, which stores all the monitoring data. In the previous version, the database was hosted by CERN central database service, but it became clear that this traffic presents a bottleneck. Furthermore, Zabbix is not well optimized on Oracle, which makes its coexistence with other database applications on a central server somewhat problematic.
- Connection to CERN Technical Infrastructure Monitoring (TIM) [3] as well as any outside Web-application is to be carried out via Oracle using a database link to the MySQL instance of Zabbix.
- Zabbix proxy servers connect to devices on the private networks of PACS, test platform of PACS, and CSAM. These proxies are implemented as virtual machines within the VSSI framework [4].
- The visualization layer based on a dedicated web-site running PHP scripts and reading data from the Oracle database has been superseded by the native Zabbix interface, which is nowadays sufficiently powerful to support such operation.

MONITORING IMPROVEMENTS

The new Zabbix version offers several improvements, which make it easier to carry out advanced monitoring tasks.

PLC Monitoring

Programmable Logic Controllers (PLCs) have been used for decades in access and safety systems at CERN. Monitoring of PLCs is important to avoid potential dangers arising from a PLC not running or its data not being updated, which can happen for example due to a loss of communication with the SCADA system.

Access and safety SCADA systems at CERN are programmed to be fault tolerant and to monitor the state-of-health of the PLCs with "heartbeats" or similar methods. However, this kind of simple monitoring doesn't always give all the information necessary. SSM monitors PLCs using 2 basic approaches.

1. Simple alive checks using standard tools like ping, traceroute, etc. These checks are already able to uncover a host of connectivity problems between servers and clients concerning faulty routers, DNS problems, and IP misconfigurations.
2. Active checks using scripts based on the LIBNODAVE libraries [5]. This method is more complex and requires special programming to get specific information from the PLCs. The most important information comes from monitoring of the diagnostic buffer, which is a ring buffer of separate diagnostic entries. In the diagnostic buffer, diagnostic events are displayed in the order of their occurrence. When the buffer is full, the oldest entry is overwritten with a new one. An analysis of this buffer provides rapid detection of causes of errors, and in case of a process stoppage, evaluation of events just prior to the problem to find the cause. Alarms are triggered for events programmed in SSM for later analyses.

Trending and Reporting

Trending has been improved in the new SSM with different screens and graphs that allow making overviews of the data giving complete information about its trends. The system allows finding patterns with correlation of graphs and screens, looking for trends that could become problems in the future, and to compare similar devices on one screen.

The Zabbix tool still has some shortcomings in certain aspects of its reporting capabilities, and specific development has been carried out to implement reports for managers and non-technical personnel. This is done by extracting the required data from the Zabbix database and plotting it using PHP and graphics libraries. Statistics and reports are produced in real-time with information about response times, errors, statistical averages, etc. An example of this is shown in Figure 1.

Figure 1: Transmit bit rates of several surveillance cameras of the SPS. Any anomalies can be spotted with a glimpse.

ISBN 978-3-95450-139-7

Trending allows isolating problems of specific hosts or discovering general infrastructure problems. It is important for maintenance planning, for dimensioning of future IT and other hardware equipment, and for spotting problems before users do. Development has also been carried out to implement trend prediction using tools like *R* [6], but this work is still ongoing.

An instructive case underlines the usefulness of trending: A trending display indicated a freak increase of network activity in a group of network-connected video cameras at night when nobody was present. The traffic subsided again in the morning. An analysis of the cameras showed that when lights were turned off at the supervised premises, the cameras went into a night-vision mode supported by many newer video devices. This then increased noise in the video images rendering the camera sleep mode inactive and causing constant dataflow to the disk servers. The problem was eventually corrected by adjusting the noise sensitivity level of the cameras.

OPC Server Interface

OPC servers are often used by SCADA systems to communicate with external clients. Data are identified by tags and read using a well-defined protocol. The original OPC server architecture is based on Windows protocols COM/DCOM, which limits access from other types of systems. A newer OPC/UA protocol is system-agnostic, but not yet universally used.

Several access and safety systems use OPC servers. In particular, the new PS access and safety systems (PACS / PASS) make most of the system data available that way. While SSM aims to interact directly with the devices themselves whenever possible, PASS devices cannot be accessed directly since they reside in an isolated private network. For this reason status data of these devices are made available on the OPC server of the PACS system.

An OPC server interface was developed using the so-called *external check* mechanism of Zabbix. The Zabbix server can call a script to run any arbitrary task that returns a meaningful value to be measured. A freely available software package, OpenOPC [7], was used to interface from the Zabbix server running Linux to an OPC server under Windows.

SNMP Interface

SNMP [8] was already supported by the old Zabbix server. However, defining SNMP items to monitor was manual work requiring finding correct tag codes from the manuals. The new SNMP builder in Zabbix is able to read an existing MIB database of a device and build monitoring rules from it directly. SNMP is used by SSM to supervise network equipment and also all the UPSs of the LACS and PACS systems.

VISUALIZATION

Visualization has been considerably improved in the new Zabbix version. It is much easier to construct custom SSM views from the monitoring data than before. In the first version of SSM these views were generated by a set of external PHP scripts, but the ability to define them directly in the monitoring tool greatly eases their management.

The maintenance and operation team has installed status screens at their premises in order to have a live view of all the systems under their responsibility. A part of this installation is shown in Figure 2.

Figure 2: Screens showing various views of the monitoring system at the premises of the maintenance team: The large screen displays the overall system status and the small screens a collection of detailed graphs. The different views have been made to rotate to display as much information as possible.

Global Views

Global views are synthesized views of the different systems offering a simple traffic-light-style view of the state-of-health of the entire system. In Figure 3 is presented the main global view of SSM. Figure 4 shows a list of active outstanding events of the entire SSM system.

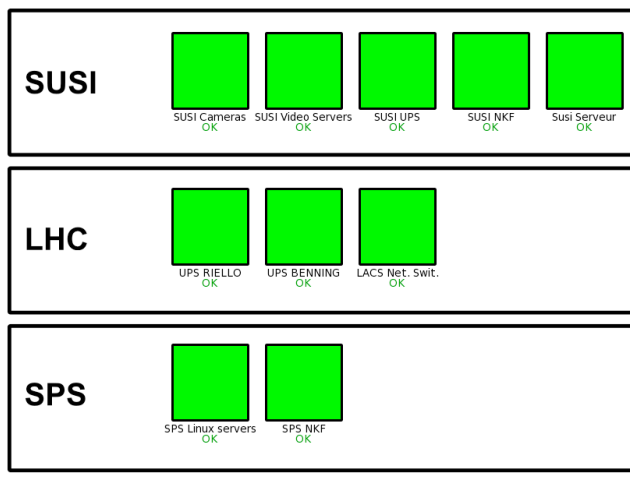

Figure 3: Global view showing the overall subsystem status of some of the access and safety systems. Green indicates that everything is ok, while red would mean that there is a problem to be investigated.

ISBN 978-3-95450-139-7

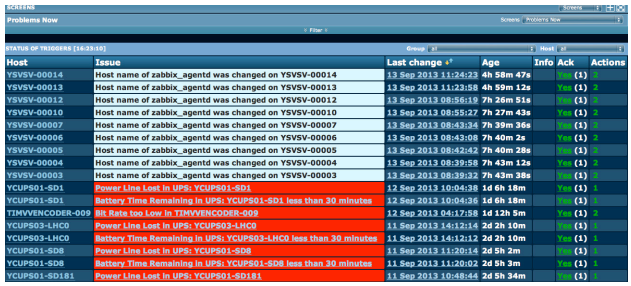

Figure 4: A global view of a list of outstanding issues in various devices. Red entries indicate critical issues requiring immediate attention.

Device Specific Views

Device specific views display details of specific subsystems or individual devices. Figures 4 and 5 show network traffic and disk utilization of several server machines.

Figure 5: Network traffic of SUSI video servers showing generally a high incoming traffic whenever an on-site camera is recording.

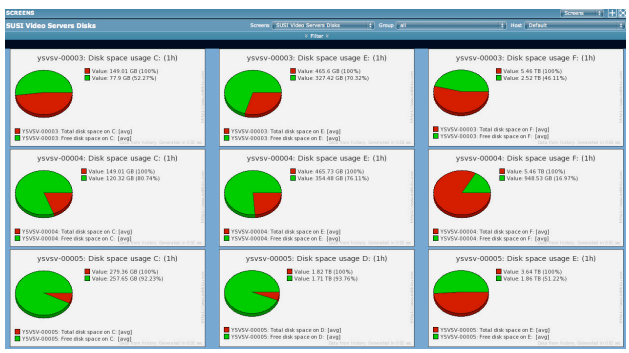

Figure 6: Disk utilization of several SUSI video servers.

Views from External Systems

It is possible to display dynamic images from external sources as web pages. Figure 6 shows a set of screen shots of SPS panel-PCs and Figure 7 several service status screens from the IT department.

Figure 7: Screen shots of the panel-PCs of the SPS access and safety system.

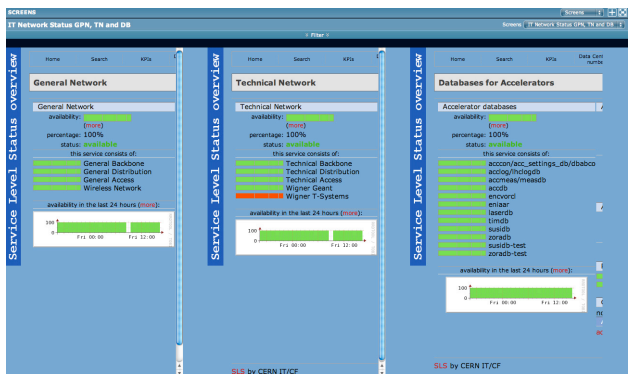

Figure 8: Status of various IT services loaded directly from the service web pages of the IT department.

CONCLUSIONS

The CERN Safety System Monitoring (SSM) system has been designed to monitor CERN safety and access systems, which are by nature very heterogeneous. A new revised system taking full advantage of a new version of the Zabbix monitoring tool is being implemented. The old and new monitoring systems will co-exist for a while during the migration process.

REFERENCES

[1] T. Hakulinen et al., "CERN Safety System Monitoring – SSM," ICALEPCS 2011, Grenoble, France, WEPMU030, p. 1134 (2011); http://www.JACoW.org
[2] http://www.zabbix.com
[3] A. Suwalska et al., "Integration, Processing, Analysis Methodologies and Tools for Ensuring High Data Quality and Rapid Data Access in the TIM Monitoring System," TUPPC029, these proceedings.
[4] T. Hakulinen et al., "Application of Virtualization to CERN Access and Safety Systems," MOPPC054, these proceedings.
[5] http://libnodave.sourceforge.net
[6] http://www.r-project.org
[7] http://openopc.sourceforge.net
[8] http://en.wikipedia.org/wiki/SNMP

ISBN 978-3-95450-139-7