CERN SAFETY SYSTEM MONITORING - SSM

T. Hakulinen, P. Ninin, F. Valentini, CERN, Geneva, Switzerland
J. Gonzalez, C. Salatko-Petryszcze, Assystem, France

Abstract

CERN SSM (Safety System Monitoring) [1] is a system for monitoring state-of-health of the various access and safety systems of the CERN site and accelerator infrastructure. The emphasis of SSM is on the needs of maintenance and system operation with the aim of providing an independent and reliable verification path of the basic operational parameters of each system. Included are all network-connected devices, such as PLCs, servers, panel displays, operator posts, etc. The basic monitoring engine of SSM is a freely available system-monitoring framework Zabbix [2], on top of which a simplified traffic-light-type web-interface has been built. The web-interface of SSM is designed to be ultra-light to facilitate access from handheld devices over slow connections. The underlying Zabbix system offers history and notification mechanisms typical of advanced monitoring systems.

INTRODUCTION

This paper presents, Safety System Monitoring (SSM), a framework for monitoring the computing infrastructure of CERN safety-related systems, such as the LHC and PS access and safety systems. While other monitoring tools exist at CERN, none of them is able to easily monitor control systems as heterogeneous as the access and safety systems.

The main purpose of SSM is 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.

MOTIVATION

In order to ensure the best possible service to their clients, access and safety maintenance teams need to know what is going on with their systems before their clients tell them. The goal of SSM is to provide the teams a straightforward remotely accessible user interface, which can help to anticipate major problems by early detection of failures. The following access and safety systems are the target of the SSM system:

- **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) – idem for the PS complex.
- **PASS** (PS Access Safety System) – idem.
- **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.

The systems themselves have normally some internal tools giving at least info on the operational status and internal state of health, as well as synoptic displays for operators and maintenance. However, there is little coherence between the different systems due to their often different approaches and levels of abstraction. The native interfaces also tend to be difficult to use requiring expert knowledge, their information cannot always be trusted due to too many layers and black-box implementation of those systems, and not everything is necessarily monitored – particularly in systems composed of many diverse components. CERN access and safety system typically consist of:

- Servers (Windows / Linux).
- Operator posts (PCs at control rooms / access service).
- Panel-PCs (local displays / information panels).
- PLCs / UTLs (local special purpose control units).
- Various other local control units.
- Video cameras / recorders.
- Biometry units (iris-scan).
- Interphones (at access points and operator rooms).
- Card readers.
- Key distributor units.
- Databases / web-servers.

These various 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 equipment reside also in the General Purpose Network (GPN) and the most important systems, in particular 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. The following basic requirements for the SSM system were identified:

- SSM would need to target directly all network-connected devices and subsystems of the systems being monitored.
- SSM needed to be easily accessible from individual PCs inside and outside of CERN.

- The adopted approach was a simple system of traffic-light style indicators (green/yellow/red) to give a quick indication of problems without going into too much detail.
- The SSM interface had to be well adapted to fixed information panel displays.
- SSM had to be easily usable with handheld devices.
- The underlying monitoring engine was to be kept separate from the visualization interface.
- It should be possible to distribute information to other systems, such as the CERN Technical Infrastructure Monitoring (TIM) [3], when this information is not available elsewhere.

A small on-paper comparison of the monitoring systems currently in use at CERN was made, and monitoring system Zabbix came out as the tool of choice [4]. The main reasons were 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 it was already known by the access and safety teams thereby making it easily acceptable.

A development project was initiated together with Assystem to develop the basic SSM application infrastructure and user interface.

DESIGN PRINCIPLES

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

- **Simplicity**: Use well-defined interfaces with clear functional separation. Use existing systems and CERN standard services whenever possible (example: Oracle, web-services, authentication).
- **Reliability**: Put in place self-diagnostic checks to tell if the displayed information is trustworthy.
- **Independency**: 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.

A division of responsibilities between system layers is based on a functional separation:

- **Collect** function: The underlying monitoring engine Zabbix carries out the actual monitoring tasks (management of local agents, connections, item logging, events, notification).
- **Synthesize** function: The integration and synthesis layer consists of a separate "scratch" Oracle database, which has access to Zabbix database tables. The database imports parts of the internal group-machine-item-trigger structure from Zabbix. All the synthesis rules for properly combining the information are defined as Oracle procedures.
- **Visualize** function: The visualization layer consists of the SSM web site [1], which accesses the synthesis database using a PHP-Oracle interface. The site is designed to be as light and simple as possible and to support both interactive and static displays.

SSM visualization layer presents information to users based on a 3-tier approach, where the roles of the different tiers are well defined:

General System Availability Tier

The general system availability tier is a generic web-based top tier presenting general status-information in the form of a synthesis of the states of various subsystems. This interface is designed to be extremely simple and light to facilitate viewing with any web browser or hand-held device (see Fig. 1).

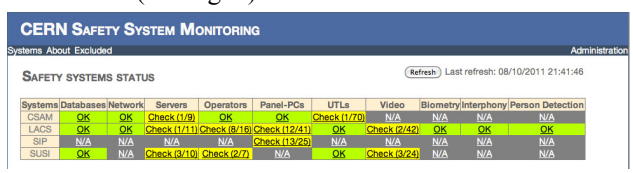

Figure 1: SSM main system synthesis view. Every monitored system is presented on a line of its own, with different subsystem categories shown as columns. Green **OK** means that everything is fine with every equipment of the subsystem, yellow **Check** means that the system continues to function but in a reduced state (non-critical failure of some equipment, with the number of failing equipment given in parenthesis), red **Down** would signify a critical failure rendering the subsystem non-operational, and grey **N/A** means that this item is not applicable to the system in question.

Subsystem Availability and Diagnostic Tier

The subsystem availability and diagnostic tier is a more detailed web-based 2nd tier allows access to a selected set of availability and diagnostic information of the various subsystems. This is simply an extension of the top tier pages allowing one to dig more deeply into the system. Similarly to the top tier, viewing of the pages is possible with the same kinds of devices (see Fig. 2).

Low-Level Diagnostic Tier

The 3rd tier comprises access to native diagnostic and configuration tools of the various subsystems. In most cases this means simply a direct link to a web-based interface of the underlying monitoring tools like Zabbix (see Fig. 3).

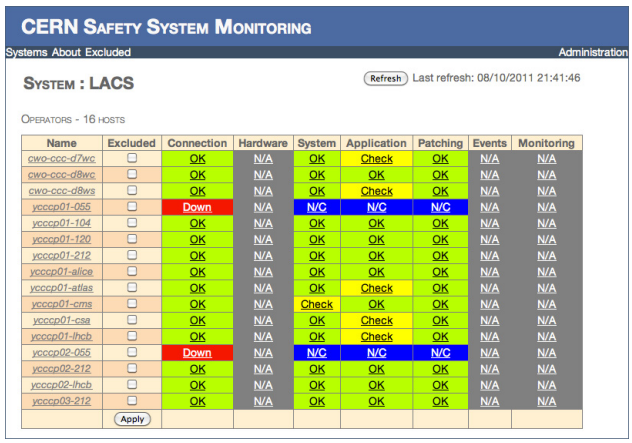

Figure 2: SSM subsystem view. All the devices of a subsystem are shown on a line of their own. The significance of the colours is the same as in the main view with addition of blue **N/C** meaning that the equipment is not communicating the information in question. The special item **Excluded** gives the possibility to mark some equipment to be excluded from the synthesis calculation (thereby not being visible in the main synthesis view) to prevent equipment undergoing maintenance or some known failures from polluting the synthesis view.

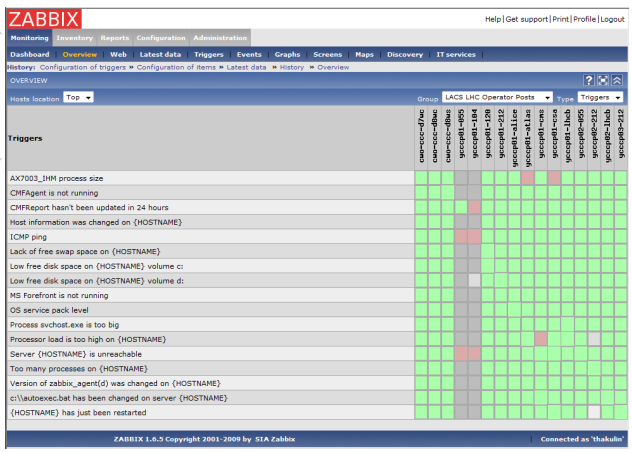

Figure 3: The native Zabbix interface. This interface permits a full access to all the features of the Zabbix tool including trend graphs, host configuration information, and email and SMS notifications. This interface is only accessible from the CERN network.

Target Audience

The expected audience of the monitoring system can be roughly divided in three categories depending on the roles and needs of each. Access to the system can be tailored to each case separately:

- **Access and safety maintenance and operation teams**. By virtue of their functions and being the main target of the monitoring system, the maintenance and operation teams have full access to all of the information and functionalities of the monitoring system.
- **Access operators, safety personnel, operational personnel, and registration service**. As the main "clients" of the access and safety systems, the operational personnel can benefit from certain elements of the monitoring system, but will probably not need access to the underlying tools.
- **CERN users and general public**. There is no interest to expose an internal monitoring system to the general public. However, some information provided by the system might become available via indirect routes, such as the information panels visible in publicly accessible areas.

Since access to the monitoring system is generally restricted to the members of the access and safety system teams and operators, an access control scheme has been implemented. This was achieved by controlling access to the web pages. There are two complementary authorization mechanisms:

- The web-server checks the ip-address of the machine where the request is coming from and if it is on the list of machines authorized to access the pages directly, access is given. These machines would include the machines running the safety information panels in stand-alone mode and possibly certain operator posts, access control configuration workstations, and dedicated terminal servers under direct control of the maintenance team or operation.
- Otherwise, a personal CERN login is requested. If the person is on the list of authorized persons, access is given. To use any configuration or diagnostic utilities with other powers besides a simple display of information, personal login is always required.

NETWORK ARCHITECTURE

The overall network architecture of SSM is presented in Figure 4. It consists of the following components:

- **Main Zabbix server**: The main monitoring engine resides in the Technical Network.
- **Proxy Zabbix server(s)**: A proxy server is a slave monitoring server for a private network able to act as an information gateway for the monitoring system between the TN and the private network segment.
- **Zabbix database:** The main monitoring data repository residing on the CERN central Oracle servers.
- **SSM database:** A "scratch" database with access to the Zabbix database and containing the synthesis rules and the data visualization logic of the SSM web interface.
- **SSMTIM database:** A second scratch database accessing the Zabbix database to distribute selected data to the TIM framework.
- **SSM web site:** A dynamic web site based on PHP scripts, which provide access to the SSM database for visualization. The web scripts contain no other logic except what is required to format and visualize the information.

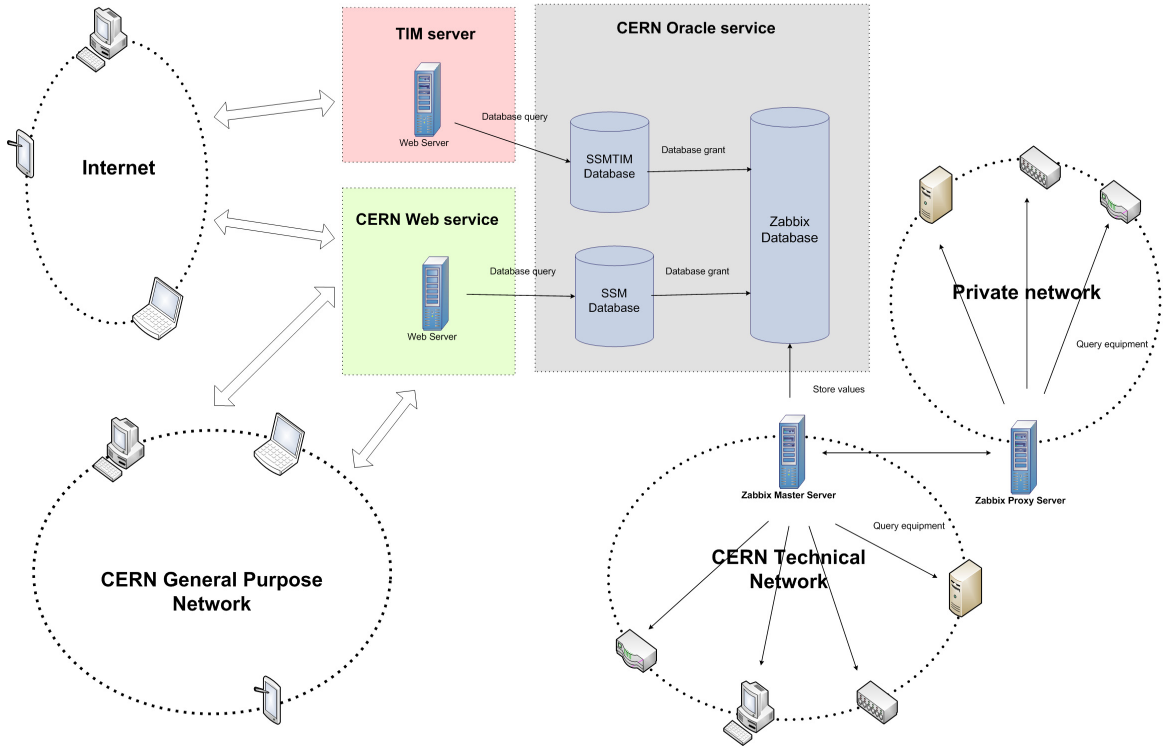

Figure 4: The overall SSM network architecture.

CURRENT STATUS

After a pilot phase of several months, SSM is in production at CERN since summer 2011. The systems integrated into the SSM are: LACS, CSAM, SUSI, and SIP. Work continues to integrate the remaining systems, SPS PSS, Sniffer, and SSA. The PS complex access and safety systems (PACS/PASS) will be integrated into the SSM framework once the renovation of those systems is final during the CERN accelerator shutdown of 2013-2014. Below are some current statistics of the SSM system today:

- 700 network connected equipment of the various systems are now monitored:
  - LACS: servers, operator posts, panel-PCs UTLs, interphones, biometry, video recorders, person detection units, network switches.
  - CSAM: servers, operator posts, panel-PCs, PLCs, network switches.
  - SUSI: servers, operator posts, UTLs, video recorders, video cameras, network card readers.
  - SIP: info screens.
  - Some small safety-related systems by other CERN teams monitored as a free service to those teams.
- 5900 monitoring items (180 new values / second).
- The full history of all values is kept for 30 days and trend data for 6 months.
- The access and safety team members have personal SSM and Zabbix user accounts to allow personal notifications via email / SMS. The authentication is via standard CERN login.
- The system has turned out to be very robust: (almost) no glitches in over a year of server uptime.

CONCLUSIONS

The CERN Safety System Monitoring (SSM) system has been designed to offer a robust and easily accessible tool for the monitoring of large scale heterogeneous systems made of numerous industrial components. It is currently under deployment on most of the CERN safety-related systems, but its open, pragmatic, and ergonomic approach based on a 3-tier user interface could be used also for the monitoring of industrial or accelerator related systems.

REFERENCES

[1] SSM web interface (CERN login required); http://cern.ch/ssm
[2] Zabbix; http://www.zabbix.com
[3] TIM (only inside the CERN network); http://timweb
[4] SSM Technical Specification; https://edms.cern.ch/document/1015740