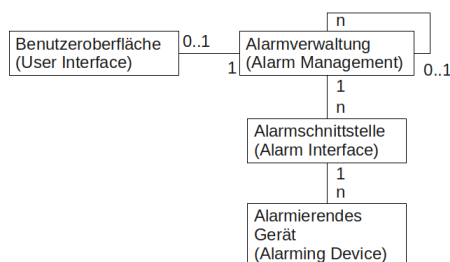


System Alarming: Eine Anwendung zur Netzwerküberwachung

WagnerTech UG, Turfstr. 18a, 81929 München, www.wagnertech.de

System Alarming ist eine systemunterstützende Funktion, die bereits seit Jahrzehnten in den Telekommunikationsnetzen für störungsfreien Betrieb sorgt. Diese Funktion sammelt Informationen über abnorme Betriebszustände und ermöglicht es so dem Wartungspersonal zielgerichtet einzugreifen, bevor es zu einem Systemversagen kommt. Als weiterer Anwendungsberich bietet sich daher die Netzwerküberwachung an. Für diesen Einsatz bietet System Alarming einen *remote watchdog*, der das regelmäßige Eintreffen von Meldungen von einem entfernten Gerät überwacht und einen *ping watchdog*, der die Erreichbarkeit eines Geräts mittels `ping` überprüft.

Die hier vorgestellte Software orientiert sich bei der Alarmbilanzierung am ITU-Standard Q.821, ohne auf alle Details einzugehen. Das System hat folgenden Aufbau:



Die zentrale Einheit von Alarming ist die Alarmverwaltung. Diese kann hierarchisch aufgebaut und auf verschiedene Knoten verteilt sein. An einer Alarmverwaltung kann eine Benutzeroberfläche angebunden sein. Die alarmierenden Geräte sind über Alarmschnittstellen an die Alarmverwaltung angeschlossen.

Die Aufgaben der Alarmverwaltung sind:

- Aufzeichnung der Alarme: Jedes Alarmereignis, das über die Alarmschnittstelle gemeldet wird, wird in einer Logdatei gespeichert.
- Bewertung der Alarme: In Abhängigkeit von einer im alarmierenden Gerät selbst erkannten Beeinträchtigung der Gesamtfunktionalität (service influence) und dem Alarmtyp bestimmt eine Bewertungslogik auf der Basis von hinterlegten Regeln die Alarmpriorität.

- Alarmweiterleitung: Da Instanzen der Alarmverwaltung hierarchisch angeordnet sein können, entscheidet die Alarmweiterleitung über ein hinterlegtes Regelwerk, welche weitere Manager zu informieren sind. Die Weiterleitung kann auch an andere Ausgabemedien, wie e-mail, erfolgen.
- Bilanzierung: Um über eine große Anzahl von Alarmen einen Überblick zu erhalten, ist es wichtig, diese zu bilanzieren. Ein Bilanzmonitor überwacht bestimmte Alarmtypen und zeigt die anliegenden Alarmprioritäten. Falls eine höhere Alarmpriorität neu hinzu kommt, stellt dies selbst wieder ein Alarmereignis dar, das an einen höher liegenden Manager weitergeleitet werden kann.
- Alarmberichte: Der Bilanzmonitor ist auch das Einstiegsobjekt zur Entstörung. Ausgehend von einer Monitorinstanz kann sich das Wartungspersonal die Einzelalarme auflisten lassen.

Um Alarme (oder *watchdog*-Ereignisse) an das System zu melden stehen folgende Schnittstellen zur Verfügung:

- SNMP (mit Paket `sysal-snmp`)
- *command line interface*: Kommandos aus dem Paket `sysal-util`
- REST-Schnittstelle

Weitere Informationen auf der Projektseite¹

¹http://wagnertech.de/?page_id=431