Semantic Alarms

Stefan Wallin Tail-f, Ph D
Director Product Strategy

Johan Nordlander, Ph D
Assistant Professor
Luleå University of Technology
Alarms, why bother?

• SDN, OpenFlow, NFV
  • 2013
• Alarms
  • 1970...

• The alarm problem is unsolved
• Alarm overload increasing
• System and network complexity increasing
Current Practice

- Syntactical Alarm
- Standards and Interfaces (X.733, 3GPP)
- Alarm Documentation Not formalized
- Correlation
- Inventory enrichment ...
- Alarms at run-time
SDN?

- OSS, BSS, Orchestration
- Logically centralized API, View
- Multi-vendor, multi-technology network
SDN – Alarms?

OSS, BSS, Orchestration ➔ Few manual actions, automation

Logically centralized API, View ➔ Synthesized Centralized Alarm Status

Multi-vendor, multi-technology network ➔ Semantic Alarm Interfaces
The SDN Control Loop

Configuration Data
Desired State

SDN

Operational Data
Actual State
The SDN Control Loop – Alarm?

Desired State ≠ Actual State

That requires Action = ALARM

Escape out of the control loop

Configuration Data
Desired State

SDN

Operational Data
Actual State
Semantic Alarm?

An Alarm signifies an *undesired state* that requires *action*.

Read the above again
- Digest...
- Undesired State!
- Requires Action!

- *Bound to the data-model for the device*
Take Action ? !

Syntactic Knowledge → Syntactic Action

Semantic Knowledge → Semantic Action
Take Action ? !
Good Alarm (EEMUA 191)?

**Characteristics of a Good Alarm**

- Relevant: i.e. not spurious or of low operational value
- Unique: i.e. not duplicating another alarm
- Timely: i.e. not long before any response is needed or too late to do anything
- Prioritised: i.e. indicating the importance that the operator deals with the problem
- Understandable: i.e. having a message which is clear and easy to understand
- Diagnostic: i.e. identifying the problem that has occurred
- Advisory: i.e. indicative of the action to be taken
- Focusing: i.e. drawing attention to the most important issues

<table>
<thead>
<tr>
<th>Long term average alarm rate in steady operation</th>
<th>Acceptability</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 1 per minute</td>
<td>Very likely to be unacceptable</td>
</tr>
<tr>
<td>One per 2 minutes</td>
<td>Likely to be over-demanding</td>
</tr>
<tr>
<td>One per 5 minutes</td>
<td>Manageable</td>
</tr>
<tr>
<td>Less than one per 10 minutes</td>
<td>Very likely to be acceptable</td>
</tr>
</tbody>
</table>
A Semantic Alarm Model

- Systems should publish the potential alarms
  - Semantic Alarm Model
- Allow for automation
  - Text-based grammar
  - YANG is *the* SDN data-modeling language for configuration, equally useful for alarm models.
- No standard for doing this
Modeling the Alarm Handling Game

enum Severity { Clear, Warning, Minor, Major, Critical }

Value operstate_t(Path) may change with each time t
Severity alarmstate_t(Path) may change with each time t
XPathExpr alarmpred(Path, Severity) static meaning of each alarm
bool istrue_t(XPathExpr) depends on operstate_t

Soundness of the alarmstate abstraction:
alarmstate_t(p) = sev
⇔
∀s ≤ sev : istrue_t(alarmpred(p, s)) & ∀s > sev : ¬istrue_t(alarmpred(p, s))
Modeling the Alarm Handling Game

Notifications sent up to time \( t \) (\( \text{Time-Path-Severity} \) triples):

\[
\text{notifs\_sent}_t = \{ (c,p,s) \mid c \leq t \& \text{alarmstate}_c(p) = s \& \text{alarmstate}_{c-\epsilon}(p) \neq s \}
\]

Notifications received up to time \( t \) (\( \text{Time-Path-Severity} \) triples):

\[
\text{notifs\_recvd}_t \subseteq \text{notifs\_sent}_t
\]

Safe interpretation of received notifications:

\[
(c,p,sev) \in \text{notifs\_recvd}_t \Rightarrow \forall s \leq \text{sev} : \text{istrue}_c(\text{alarmpred}(p,s)) \& \forall s > \text{sev} : \neg\text{istrue}_c(\text{alarmpred}(p,s))
\]
Summary

Alarms are an operational pain

Less Alarms
Less Manual Work
More Automation

We need a standard to express these

Semantic Alarm Models
See also....

- 3GPP TR 32.859 Study on Alarm Management
  - Tommy Berggren, TeliaSonera
- “Chasing a Definition of Alarm”
  - Stefan Wallin
  - Journal of Network and Systems Management
  - Volume 17 Issue 4, December 2009
- “The semantics of alarm definitions: enabling systematic reasoning about alarms”
  - Stefan Wallin, Johan Nordlander, Viktor Leijon, Nicklas Bystedt
  - International Journal of Network Management