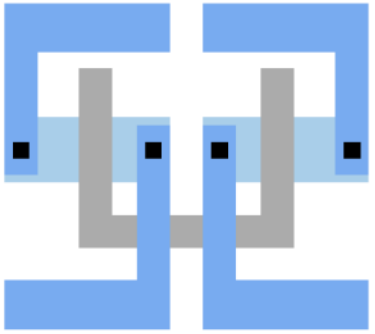
UNIVERSITÄT
HEIDELBERG

Alarm System

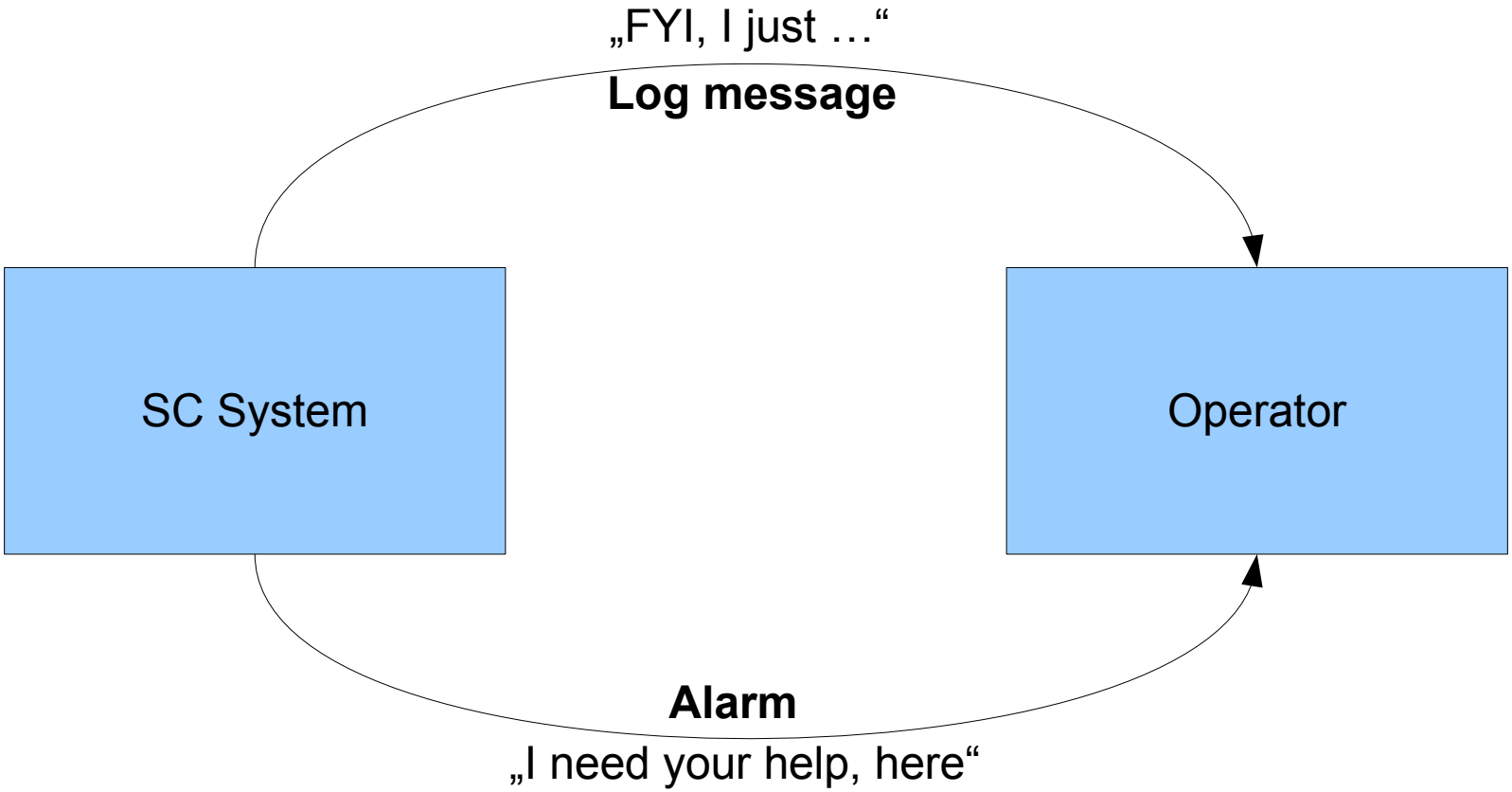


Michael Ritzert

michael.ritzert@ziti.uni-heidelberg.de

19.12.2018

Handling of Problems in the SC System



- Problems that can be resolved automatically
  ⇒ Just do it. Tell the operator via a log messages about what just happened.
- Problems that cannot be resolved automatically
  ⇒ Raise an alarm to let the operator deal with it.

What is an Alarm?

Naive approach:
If what comes out is not what I commanded, that's a problem.
⇒ This is what would happen:

Power Supply		
Set Voltage	**Current Voltage**	
1.8V	**1.8V**	**all well**
1.8V	**2.0V**	**wrong voltage**
1.8V	**1.5V**	**wrong voltage**
1.8V	**0V**	**wrong voltage**

Very simple to implement: Set != Current (+/- Delta) => Alarm.
But this doesn't always highlight the cause of the problems.

What is an Alarm?

Power Supply

Channel	Set Voltage	Set Current	Current Voltage	Current Current	
on	1.8V	100mA	1.8V	10mA	all well
on	1.8V	100mA	2.0V	10mA	wrong voltage
on	1.8V	100mA	1.5V	10mA	wrong voltag
on	1.8V	100mA	1.5V	100mA	wrong current
off	1.8V	100mA	0V	0mA	all well

⇒ even in this simple case, the condition is complex:
The voltage is in error,

- if it is lower than the set voltage, but not
  - if the PS is switched off, or
  - if the PS is in the current-limit mode.
- or if it is higher than the set voltage.

⇒ Important: what is **expected** to happen? In current-limit mode, the voltage is expected to drop. The problem is only in the current.
⇒ Defining when a condition is **not** an alarm is very important.

Definition

- Alarm: An **unexpected state** of the system that **requires operator intervention**.

- Clear definition of severities:
  - Major: system **is** broken.
  - Minor: act **now**, or system **will** break.

  ⇒ There cannot be a minor alarm without a major alarm.

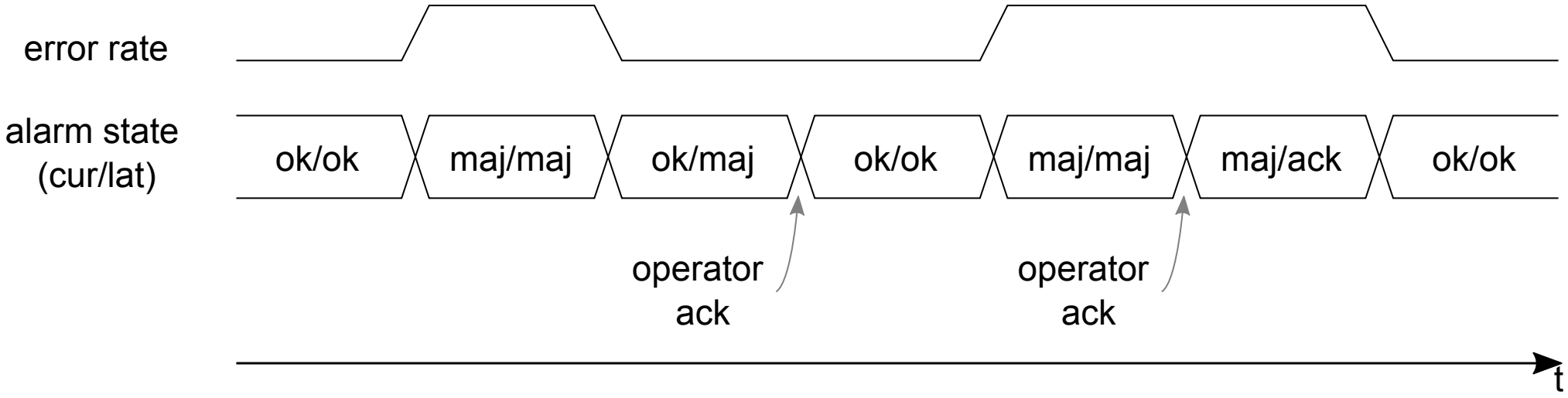
  ⇒ „This is really bad“ or „that's not that bad after all“ are **not** the definitions of major and minor.
- If the failure is unavoidable, the severity is major right away.

Alarms Must Be …

- Relevant for the shifter.
- Non-redundant: Only one alarm per error situation.
- Latching: No alarm may just disappear by itself.
  The operator always needs to acknowledge it.
  Two situations:
  - Condition can disappear without operator action (e.g. overtemperature)
    ⇒ Must be latching in the alarm server (default).
    (Should be rare, given that an alarm is a predecessor of guaranteed failure.)
  - Condition needs to be cleared manually (e.g. PS OVP trigger: requires OVP reset).
    ⇒ This manual operator action counts as the acknowledment
    ⇒ Alarm can be non-latching in the alarm system.

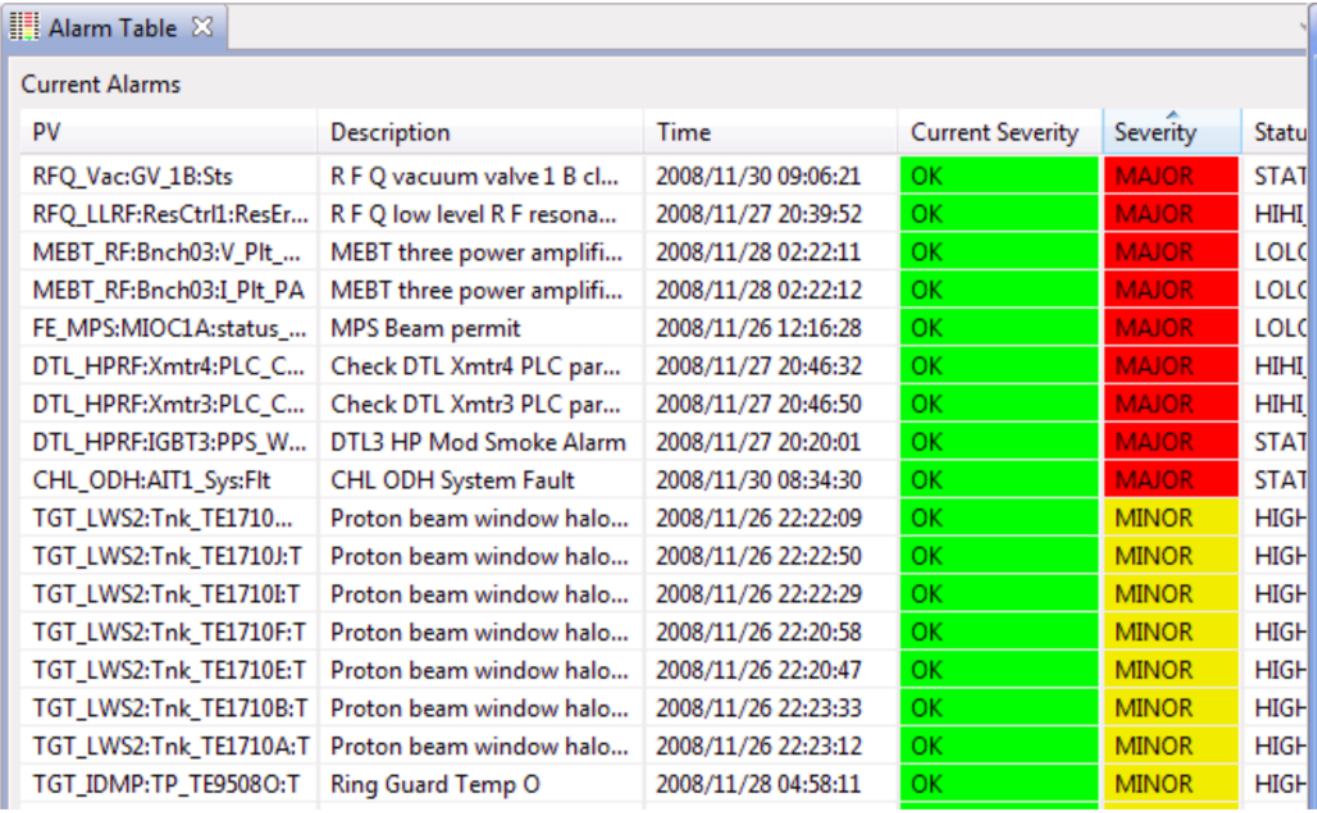
Alarm System I

- The Best Ever Alarm System Toolkit, a.k.a. **BEAST.**
- Manages alarm conditions in a tree-like structure, propagating alarms up to the root.
- Two states per alarm:
  - current condition, live from the PV
  - „latched“ condition: worst condition since last alarm acknowledge.
- Example alarm lifecycle:



Alarm System II

- The alarm server is a standalone executable
  ⇒ operates independently, backed by a PostgreSQL database.
- In CSS, the alarm module is used to display the alarm.
  - Displays as a tree, or as a table.
- Notifications by mail, sound in the control room are possible.



Thank you!