

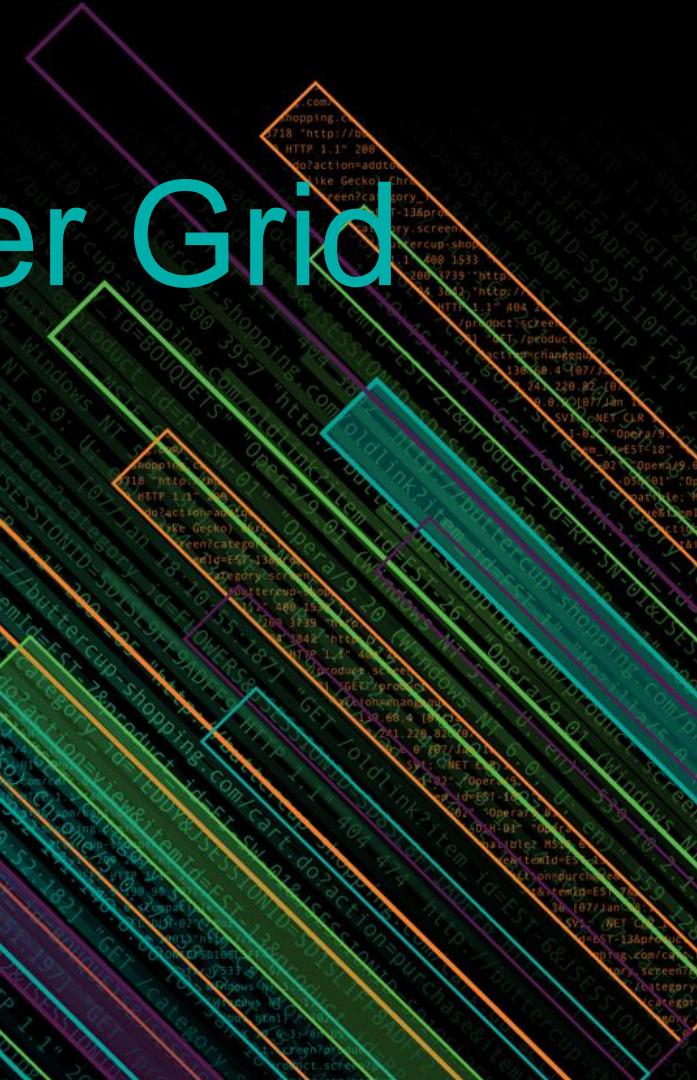


splunk>

Monitoring a National Power Grid With Splunk and ITSI

Linus Myrefelt, Statnett Splunk Ninja

October 2018



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

No Photos

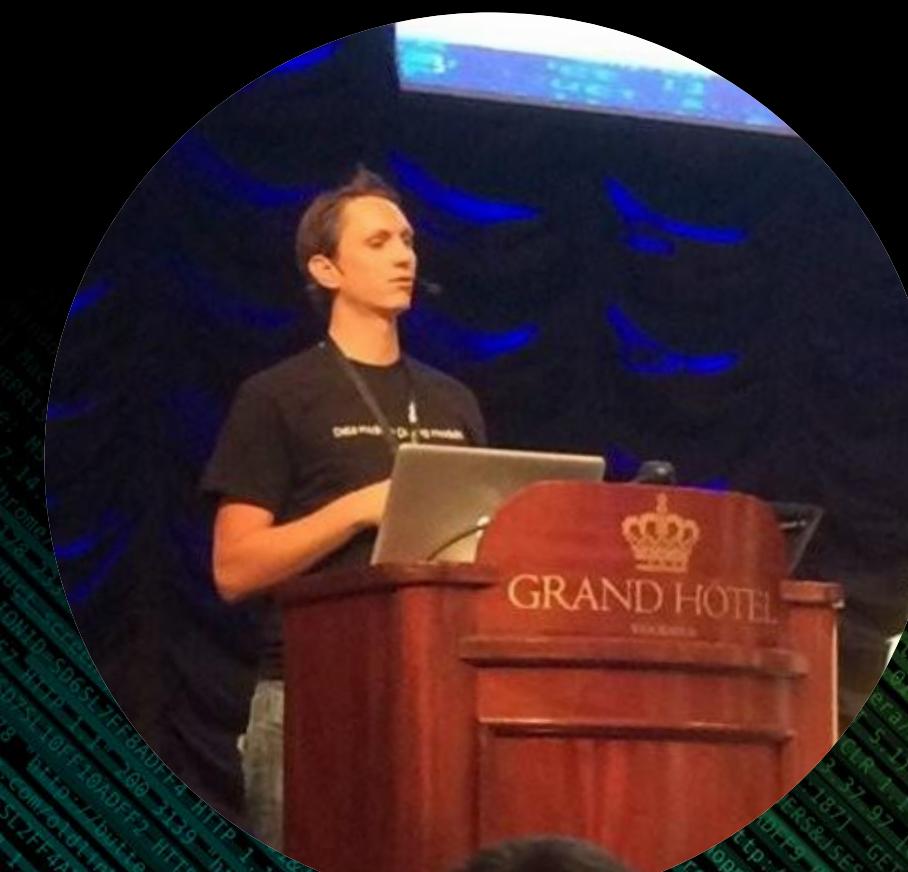
This deck contains proprietary information,
no photos or video recording please!

Agenda

1. Introduction
2. Monitoring the National Power Grid Using Splunk
3. IoT in the OT World
4. The Road to Splunk ITSI
5. Lessons Learned

LINUS MYREFELT

Statnett Splunk Ninja



MY BETTER SELF

My Mini Me



splunk> .conf18



Statnett

What is EMS?

▶ EMS

- Also a term SCADA/EMS is used) supervises, controls, optimizes, and manages generation and transmission systems
 - EMS enables utilities to collect, store, and analyze data from hundreds of thousands of data points in national or regional power systems, perform system modeling, simulate power operation, pinpoint faults, preempt outages, and participate in energy trading markets

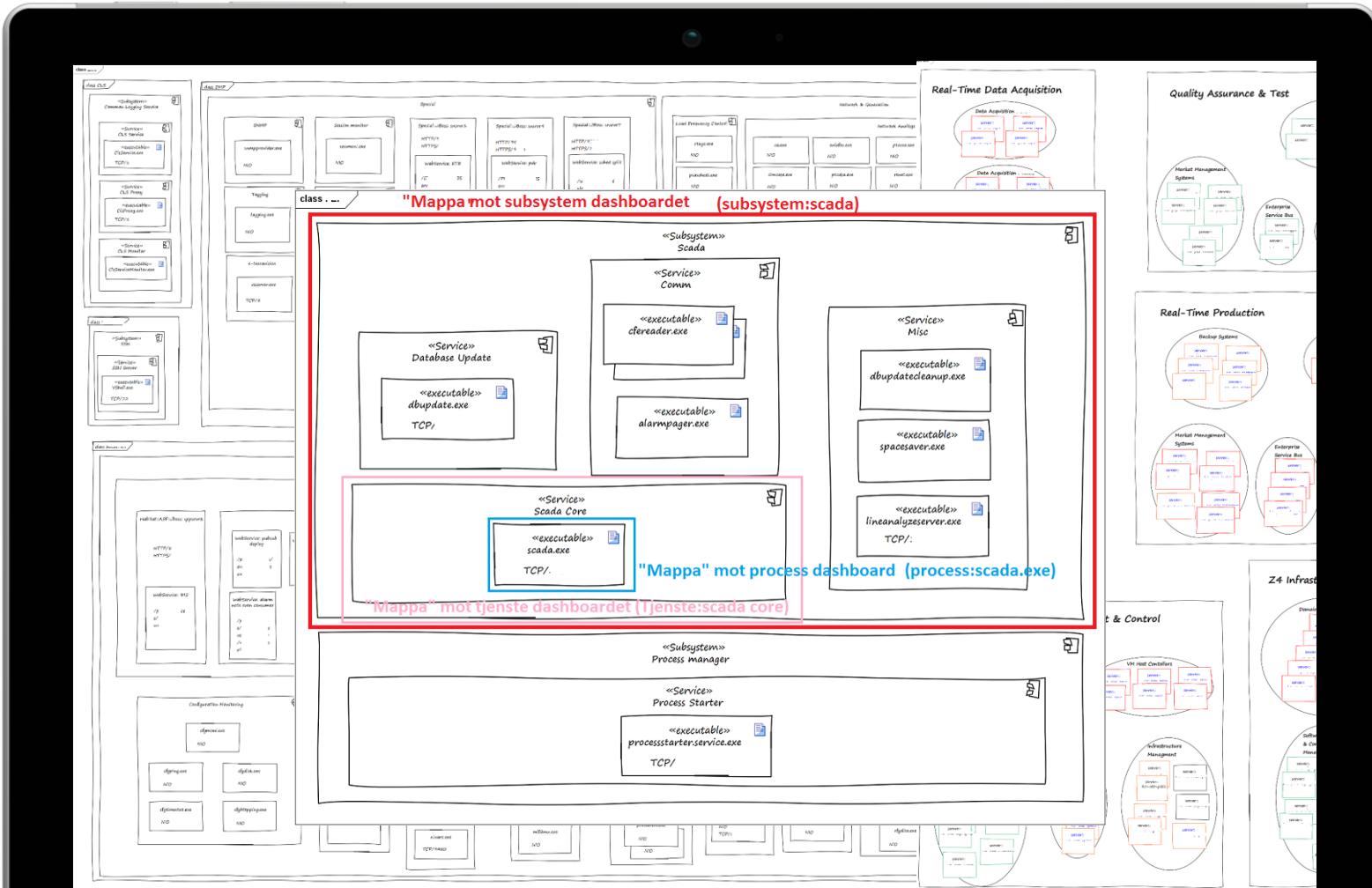






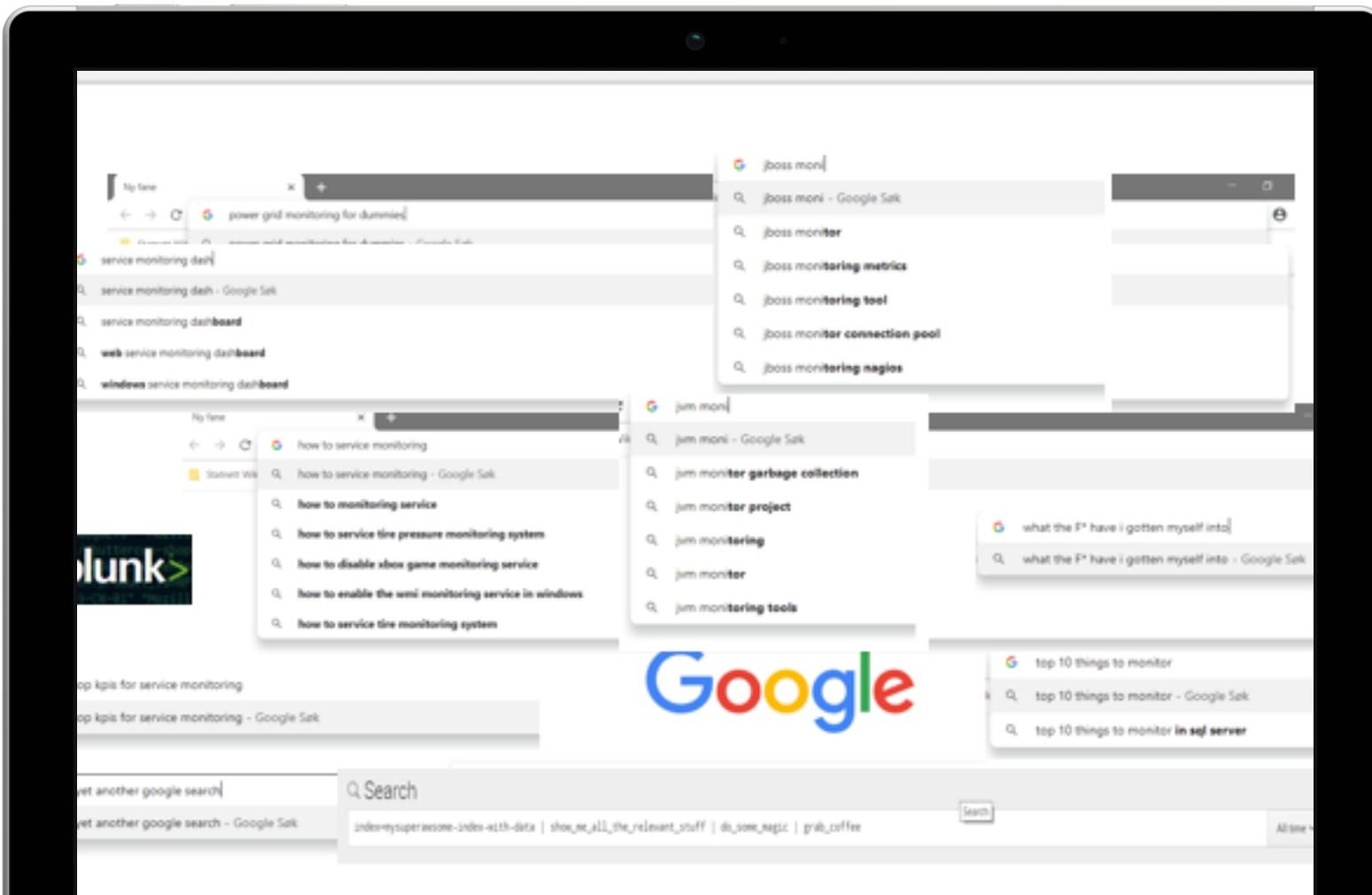


Input and Data Sources



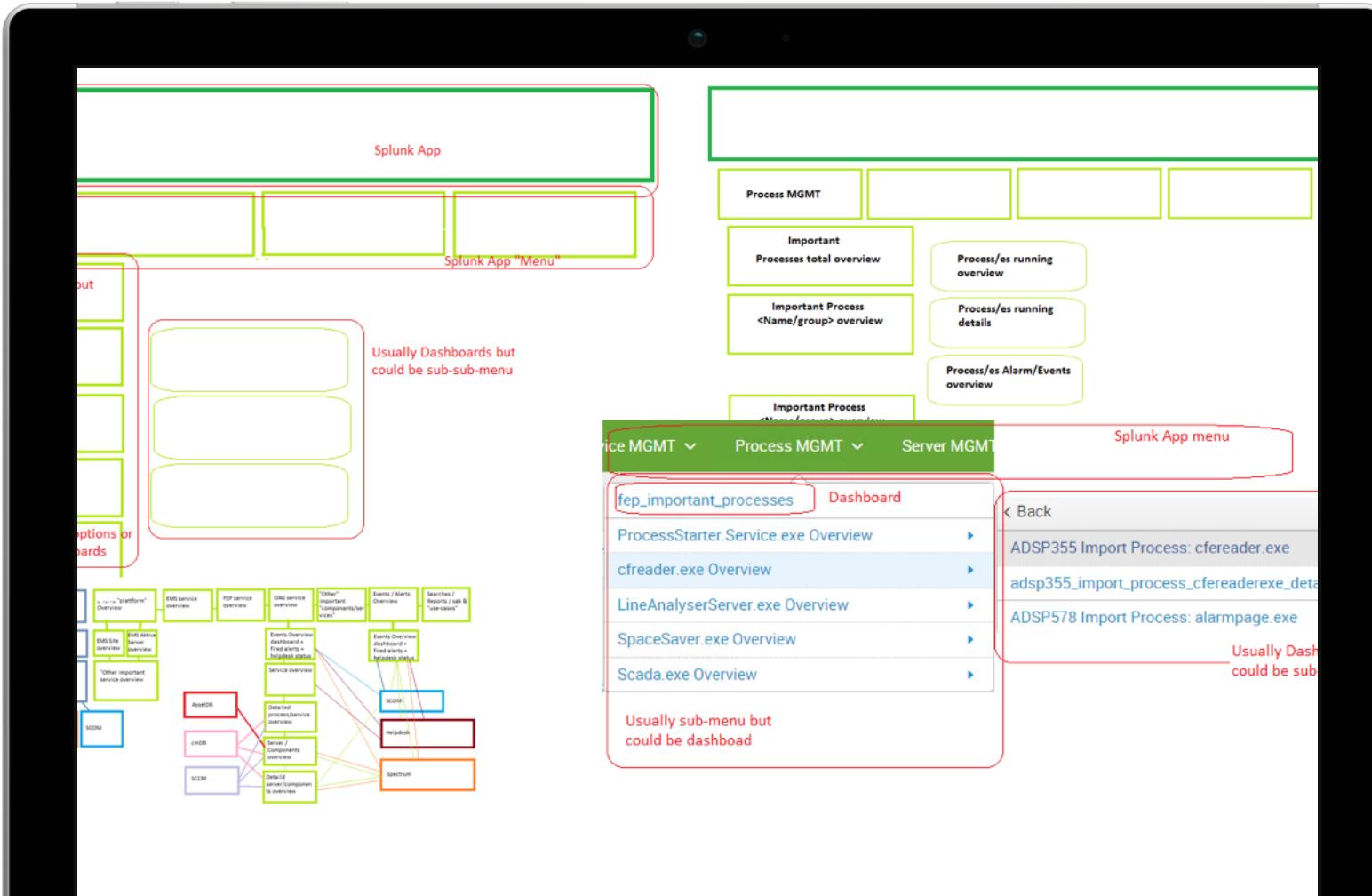
- Inputs
- System diagram
- Platform diagram
- Network / service architecture diagram
- Excel sheet with important processes / message codes / "metadata"
- Screenshots

Research Phase



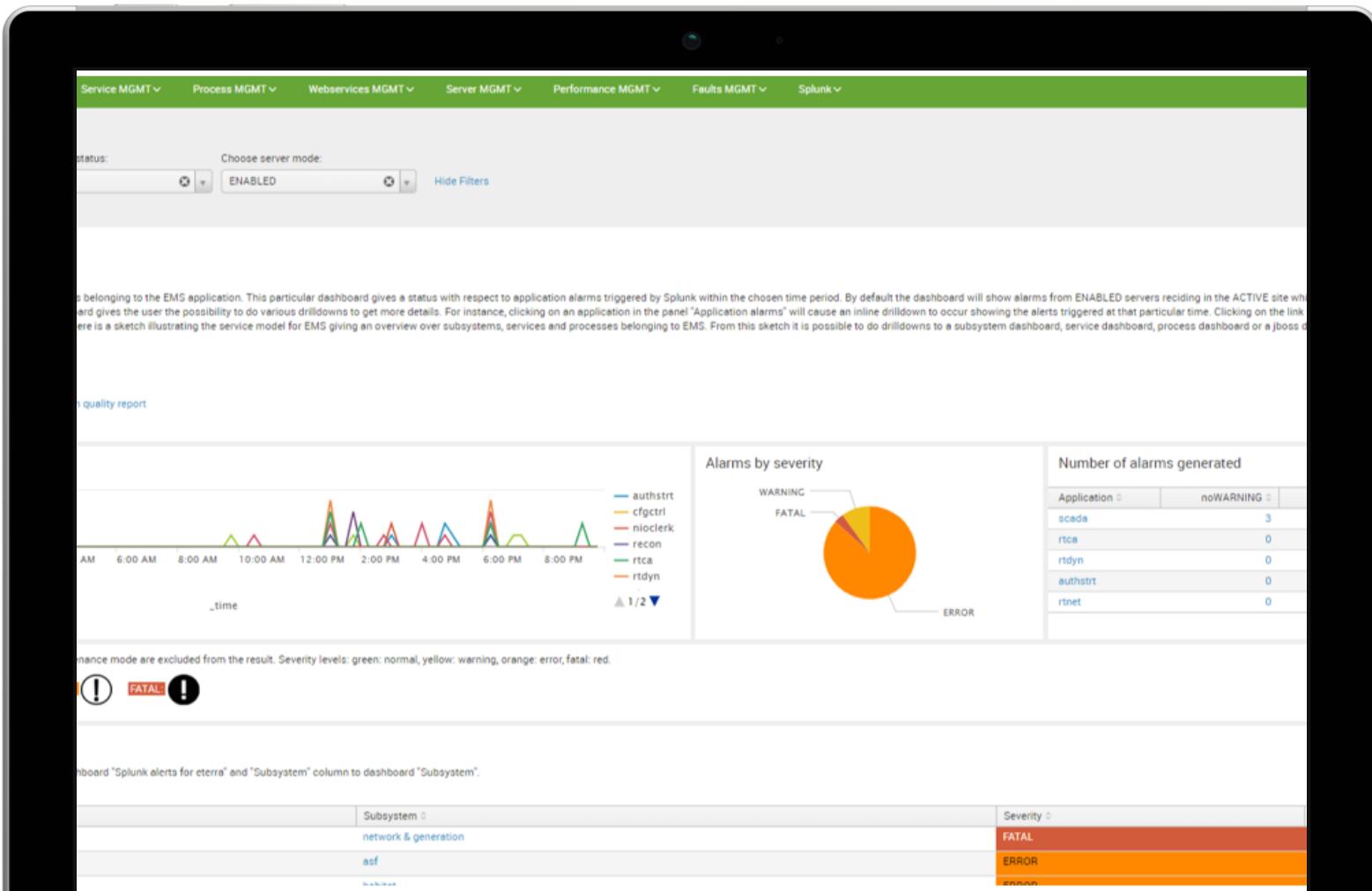
- ▶ Define what a service is and its various states
- ▶ Define requirement for monitoring
 - Utilization
 - Server Monitoring
 - Can we correlate this?
 - Other monitoring tools?

Developing Splunk Apps



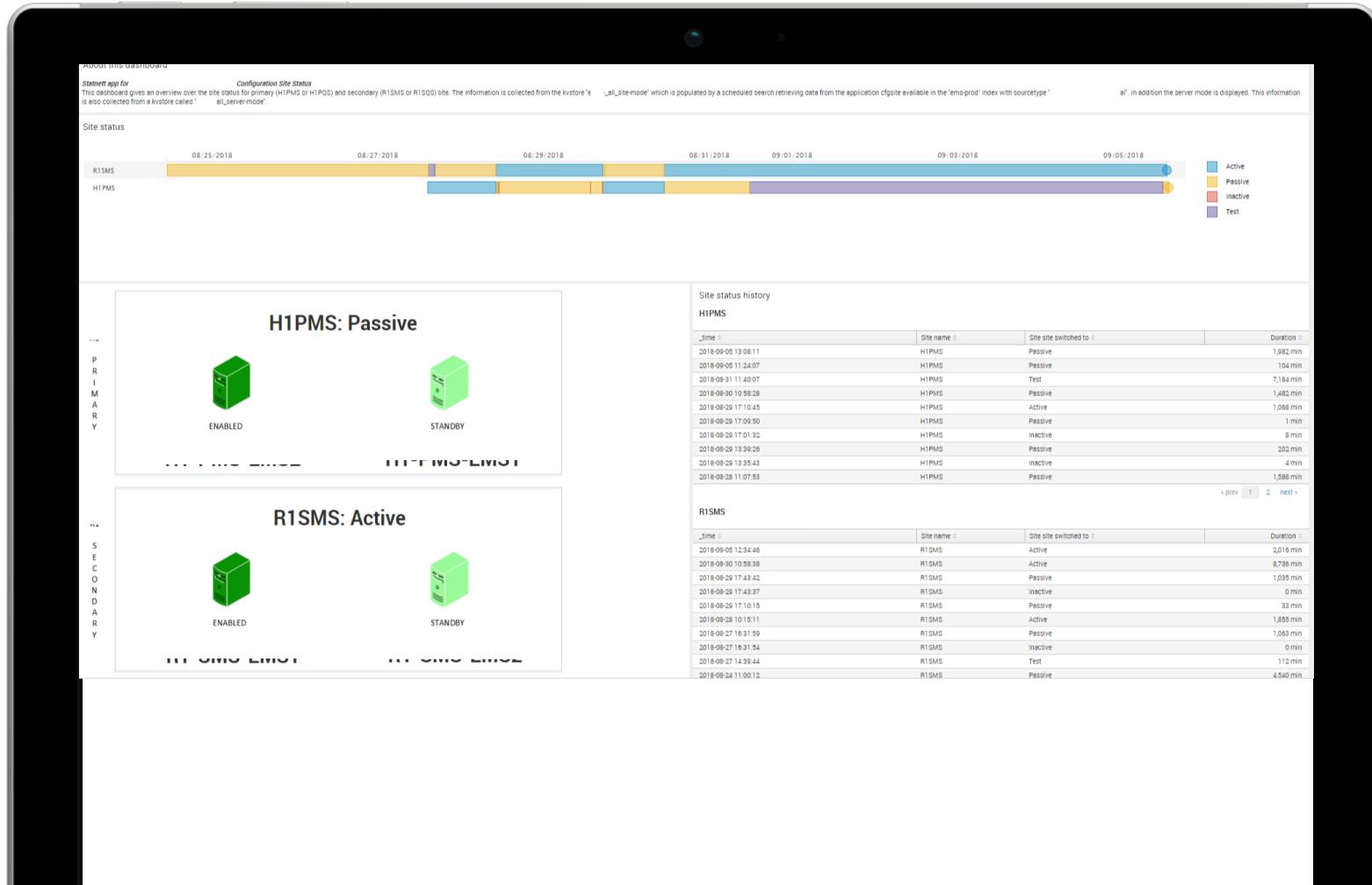
- ▶ Create mockups before
- ▶ We created a handful of “apps” separated by role and function
- ▶ We wanted a high level subsystem view and detailed service view

The Results



- ▶ This is the start page of each Splunk App
- ▶ Contain the most necessary information
- ▶ While also enables you to drill down into the details and alerts
- ▶ Bridges together the IT/OT environments

The Results



- ▶ Contain info and stats around node and site failure with the EMS
- ▶ State of system helps to dictate urgency
- ▶ Use lots of lookups and KV Collections to monitor the state

The Results

About this dashboard

Processes for subsystem: scada

Service	Process	Description
opencalc	opencalc.exe	Allows end-users to create calculations on the fly
scada	proxysrv.exe	ISO communications take place over a pair of NETIO paths (one for data and one for controls). In the case of front ends, PROXYSRV running on the EMS server converts connection requests from front ends (e-terracontrol) into NETIO "open path" requests. Once the connection from the front end to the proxy task and the corresponding NETIO connection from proxysrv to the EMS SCADA task are formed, then communication takes place.
comm to fep		
scada comm to gpsclock	scadafreq.exe	SCADAFREQ software is responsible for interfacing with TrueTime Frequency Devices, in order to gather frequency-related information and deposit it in the e-terrascada database.
scada core	scada.exe	SCADA: Primary data task, including data acquisition, supervisory control, and online editing. The SCADA task also handles transfer of intersite measurement data to and from remote sites, as well as historical data recording.
scada core	scsrv.exe	SCSRV: This is the e-terrascada Application Programming Interface (SCAPI) server task. It allows access to the e-terrascada database from other applications. It is also a TAGGING API client to populate SCADAMON database with tag properties.
scada misc	css.exe	The Control Sequence Scheduler (CSS) application is used to provide the ability to add, modify, and execute sequences of supervisory controls at scheduled times.
scada misc	fedownload.exe	FEDOWNLOAD: This is the task that dynamically creates and transfers incremental database changes to the appropriate e-terracontrol front ends for automatic application of changes.
scada misc	hdrcopy.exe	HDR Copy Files to Backup Disk directory. Used to maintain redundancy on the short term history
scada misc	recon.exe	*** Description missing ***
Scada misc	scadatop.exe	SCADATOP: e-terrascada Topology processing provides the functionality of Topology Processing for producing alarms and driving topology information about one-line displays. The SCADATOP task uses the e-terrascada API (SCAPI) interface for retrieving e-terrascada data.

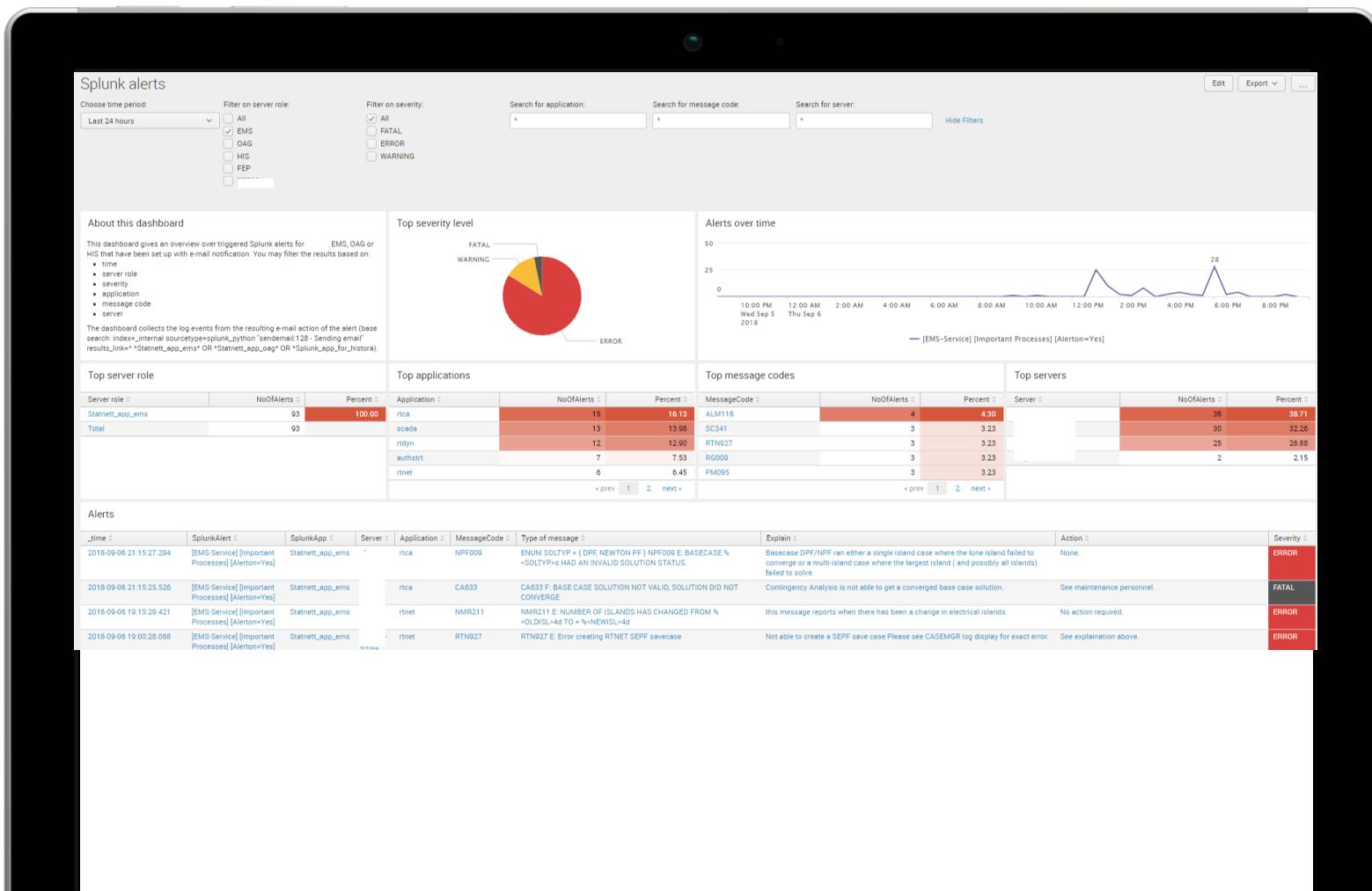
Subsystem -> Service -> Process diagram

Status of subsystem: scada

Server	Region	CurrentMode	Site state	OldestEvent	LatestEvent	RunningProcesses	Status
		STANDBY	Passive	2018-09-06 21:35:49	2018-09-06 21:45:49	css.exe fedownload.exe hdrcopy.exe opencalc.exe proxysrv.exe	OK

- ▶ Subservice dashboard contains description
- ▶ Higher level information is a "defined" subsystem

The Results



- ▶ Centralized overview of alerts generated from Splunk

Application and Process-Focused Dashboard

The screenshot shows a Splunk-based dashboard titled "Important processes for EMS". The top navigation bar includes links for Start, Search, SubSystem MGMT, Service MGMT, Process MGMT, Webservices MGMT, Server MGMT, Performance MGMT, Faults MGMT, and Splunk. The dashboard has several filter sections at the top:

- Choose time period: Last 15 minutes
- Choose region: All (*)
- Choose environment: real-time production
- Choose type: ems servers
- Search for server: (empty)
- Search for process: (empty)
- Choose process criticality: U, H, M, L (checkboxes checked for U and H)
- Choose process state: P, E, S, O, T, D (checkboxes checked for P and E)

About this dashboard:
This dashboard gives an overview over important processes for Statnett_app_ems. You filter the results based on time, server, process and the criticality and state defined for the process.

Important processes:
Source: lookup _all_server-roles_2_apps_state_n_criticality.csv

Process	Application	Criticality	State	Description
alarm.exe	alarm	H	P	IMAGE Alarm
authstrt.exe	authstrt	U	P	AUTHSTRT: Authorize ETP Startup
ca.exe	rta	H	P	Real-time Contingency Analysis
cfgctrl.exe	cfgctrl	U	P	CFGMAN Control Task
cfgsite.exe	cfgsite	U	P	CFGSITE Task

No results found.

Explanation of criticality:
Source: lookup _app_states_2_desc_N_severity.csv

Explanation of state:
Source: lookup app_states_description.csv

State	Description
P	Permanent => the application should always run : down = trouble
E	Enabled => the application runs only if the server is in Enable : down = trouble
S	Standby => the application runs only if the server is in Standby : down = trouble
O	Occasional => it is not meant to run
T	Transitory => the program execute a task and ends when the task finish
D	Disabled => should not run

Status per server:

Server	CurrentMode	OldestEvent	LatestEvent	RunningProcesses	ProcessesNotRunning	Status
STANDBY	2018-09-06 21:50:49	2018-09-06 22:04:49		alarm.exe authstrt.exe ca.exe cfgctrl.exe rta.exe	trend.exe	NOT OK

- ▶ Centralized overview of Processes

Sample Report



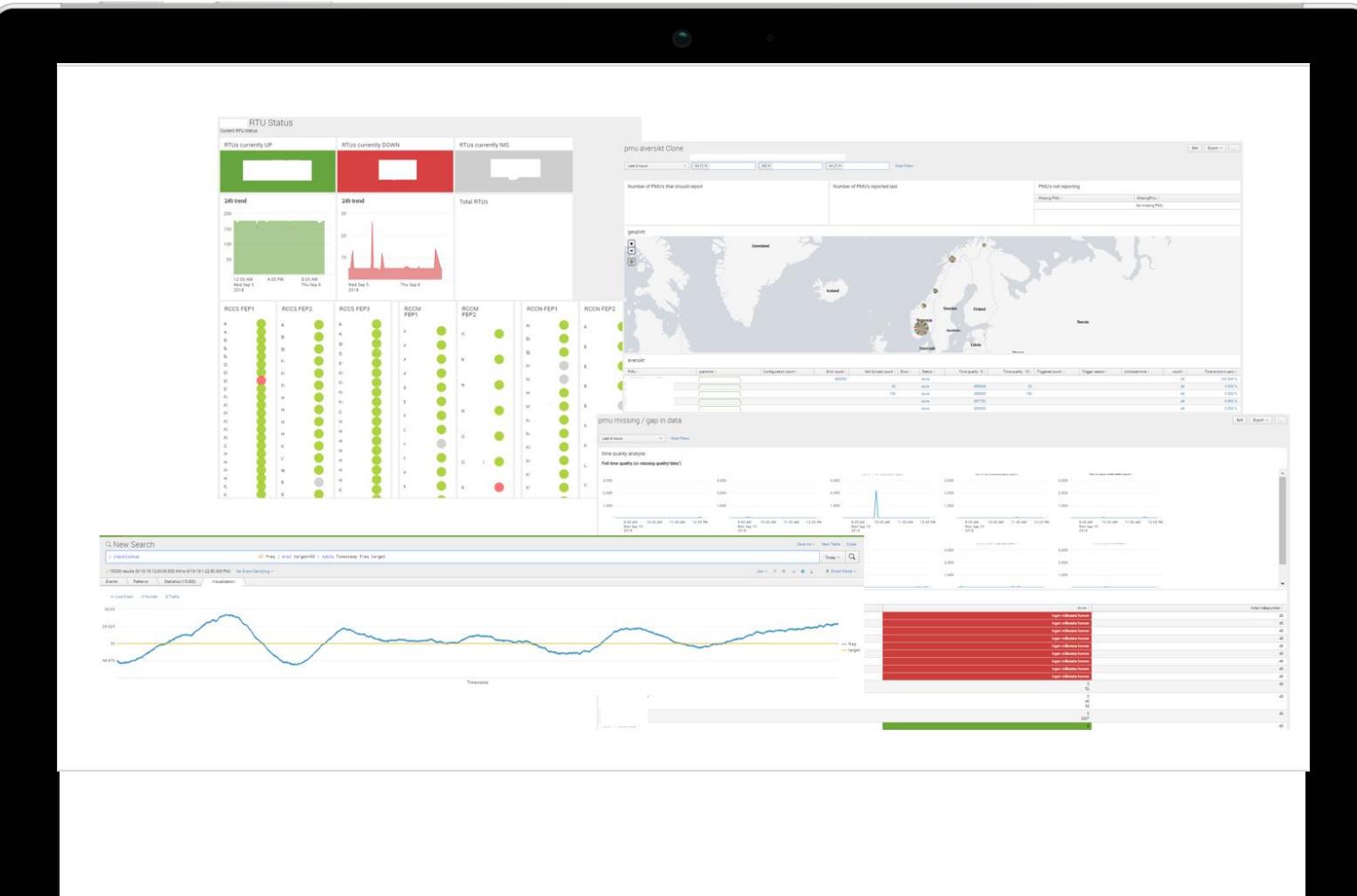
- ▶ Example of report generated based on collected scada data

IoT in the OT World



- ▶ RTU: Remote terminal unit
 - Collects and transfers data
 - Responds to and executes commands and order the EMS
 - ▶ PMU: Phasor measurement unit
 - A device which measures the electrical waves on an electricity grid using a common time source

IoT Dashboard

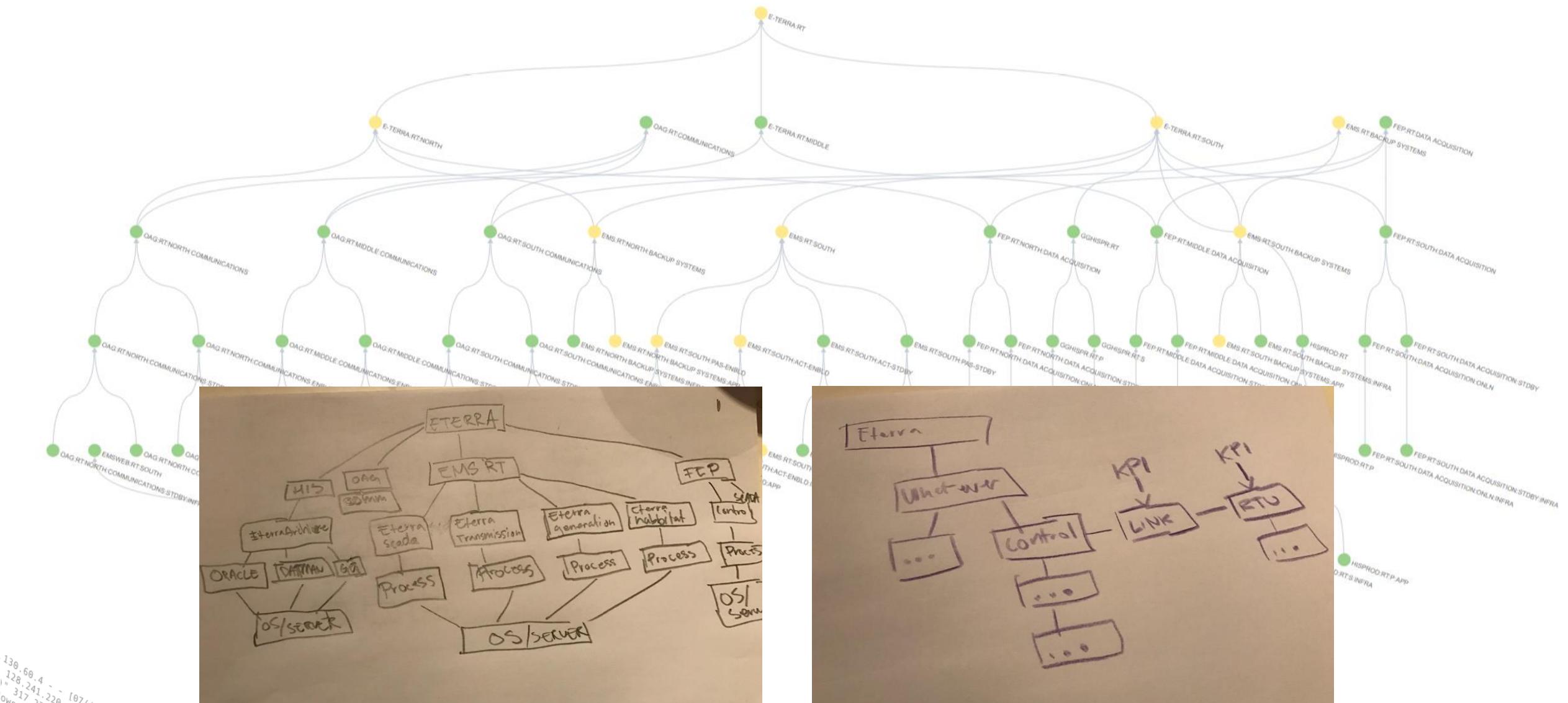


► Yay, we do IoT stuff

The Road to ITSI Enlightenment



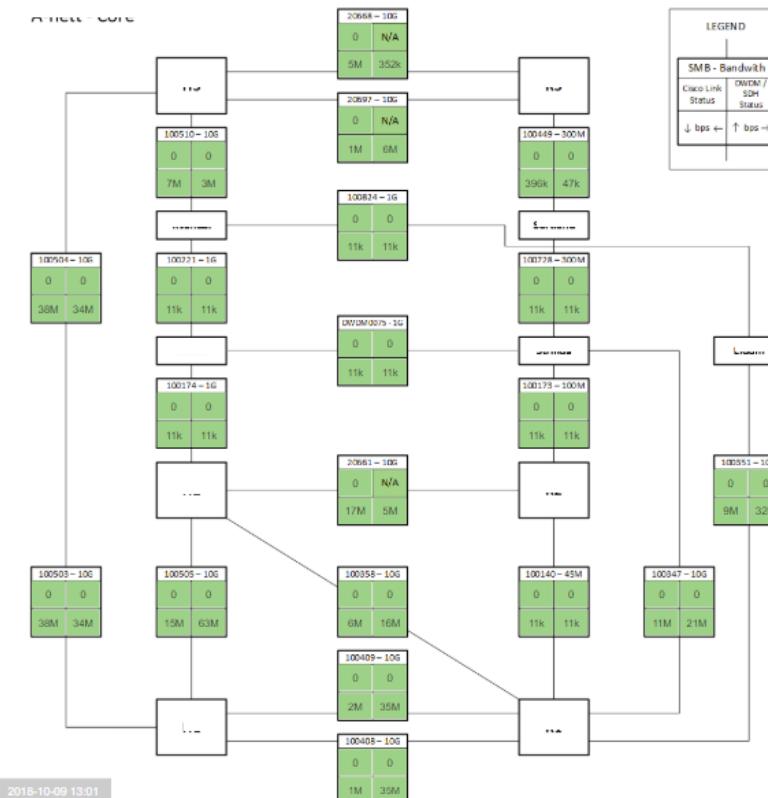
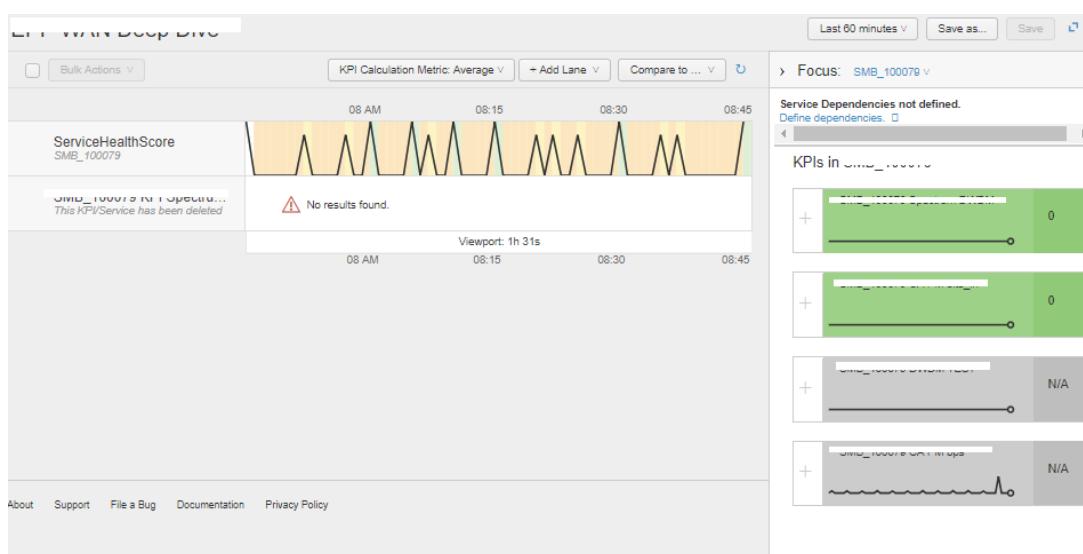
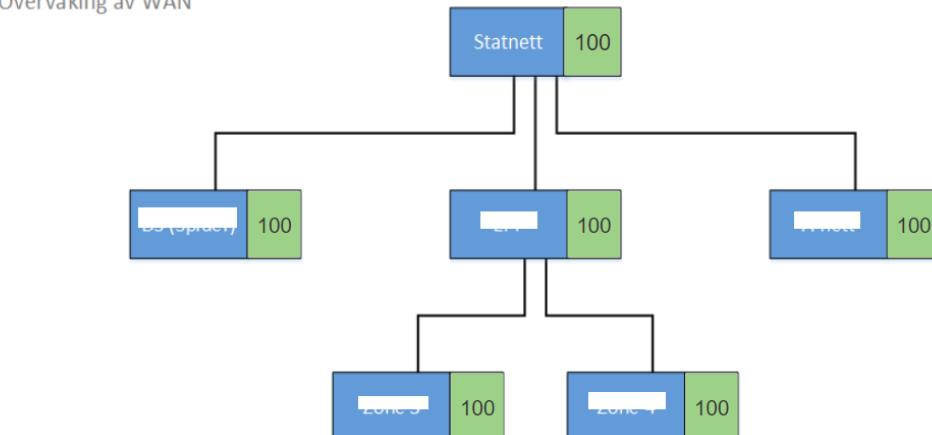
ITSI Mock-ups



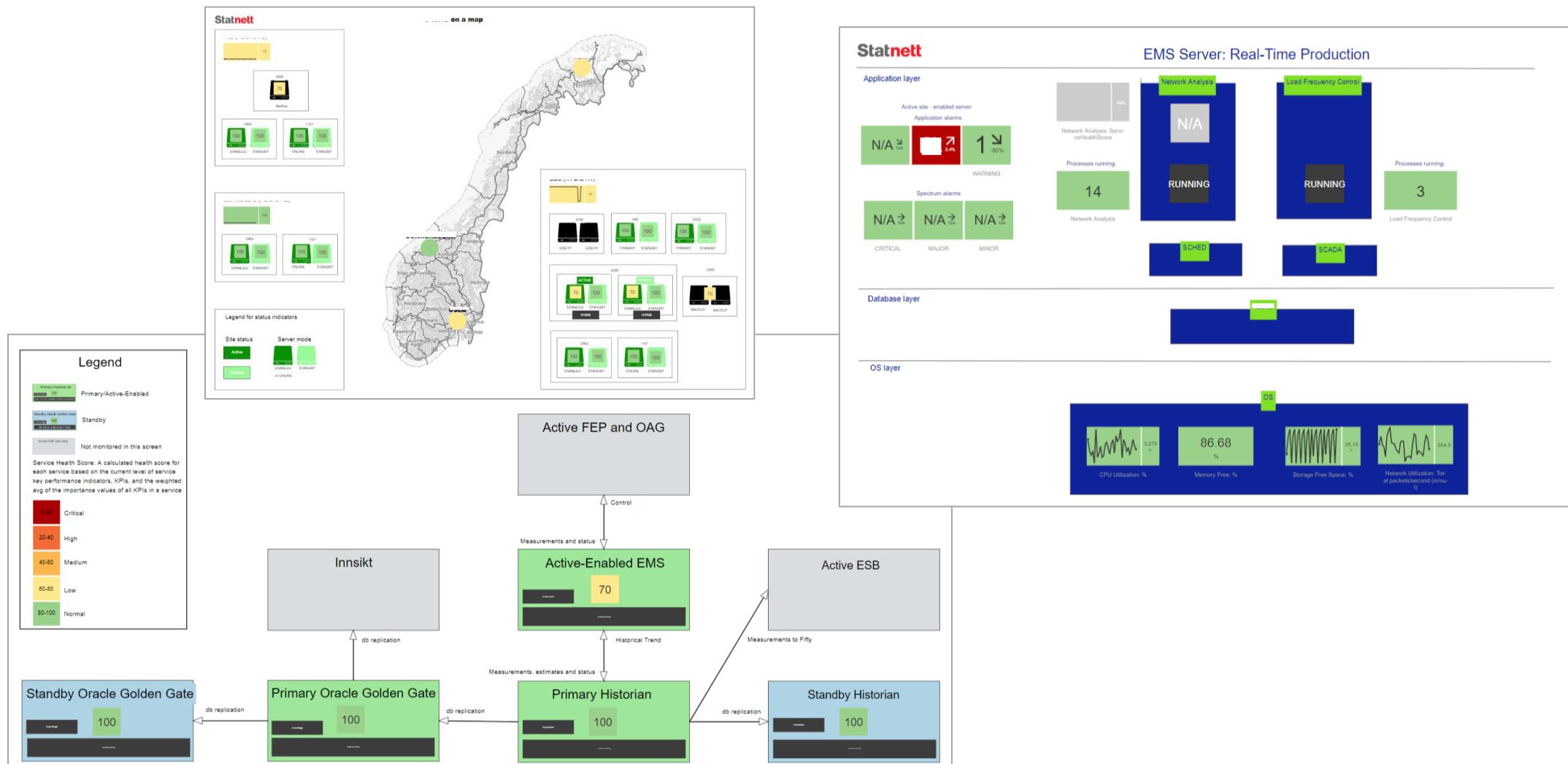
Infrastructure Glass Table Examples

Statnett

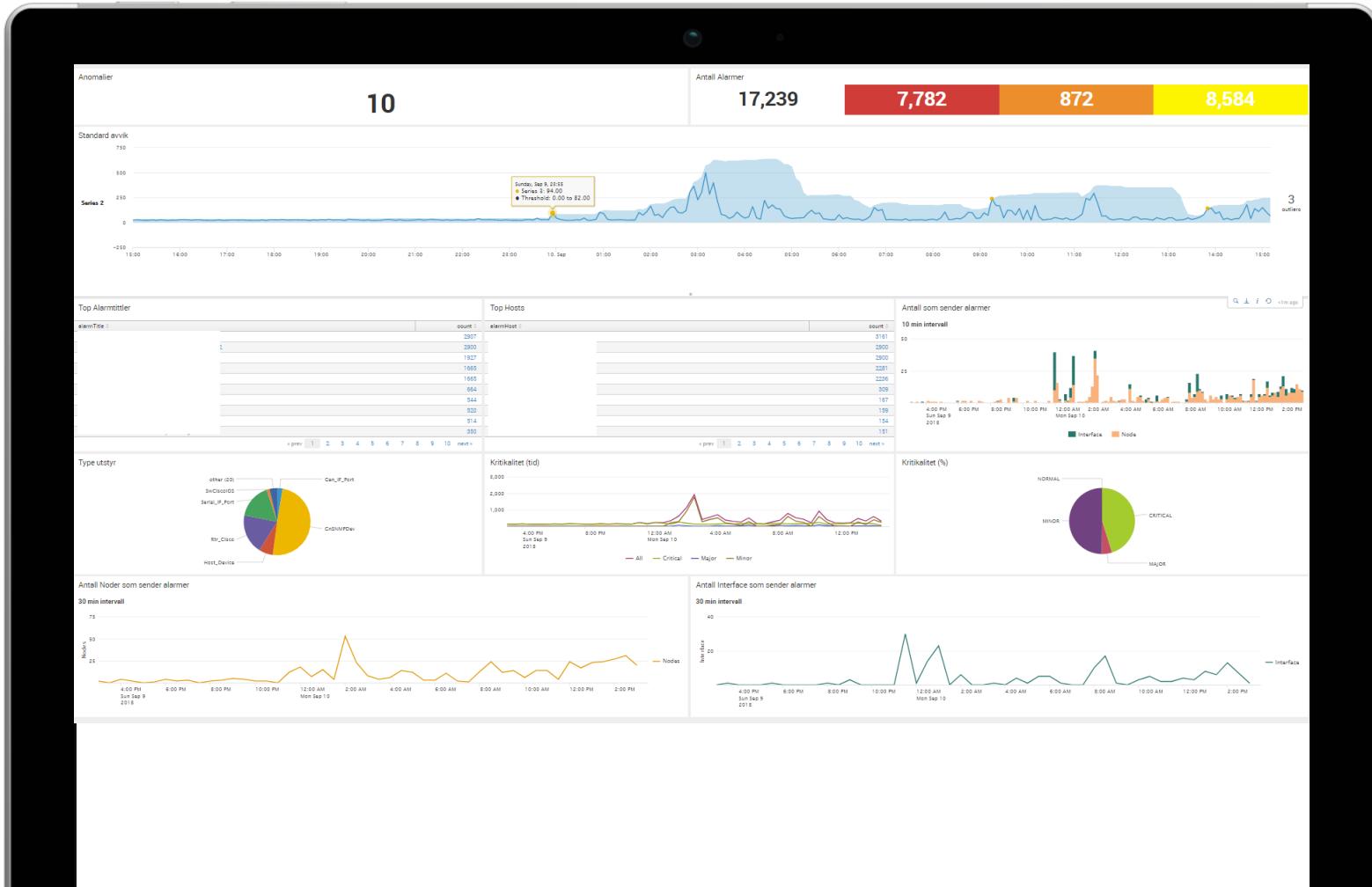
Overvåking av WAN



Scada Focused Glass Tables



Machine Learning and Lessons Learned



- ▶ Playing around with Machine Learning

Lessons Learned



Thank You!

Don't forget to rate this session
in the .conf18 mobile app

.conf18
splunk>

