# Centralized Logging and Alerts for EPICS-based Control Systems With Logstash and Grafana

Ken Lauer [1] – klauer@slac.stanford.edu

1. SLAC National Accelerator Laboratory, USA

## OVERVIEW

Controls-focused centralized logging on the experimental side of the LCLS aims to bring together logging information from a variety of disparate sources into a single database for easy correlation and alerting.

Our application of EPICS covers thousands of IOCs, dozens of Channel Access gateways, hundreds of PLCs and other physical devices, and numerous user-facing applications all running simultaneously.

## HIGH-LEVEL VIEW

Application exceptions + logs with standard library logging via pcdsutils

Library, program and system logs using lcls-twincat-general and ads-log-daemon

IOC Logs
IOC caPutLogs
Channel Access Gateway put logs

Archiver Appliance

archstats

Logstash

Grafana

Elasticsearch

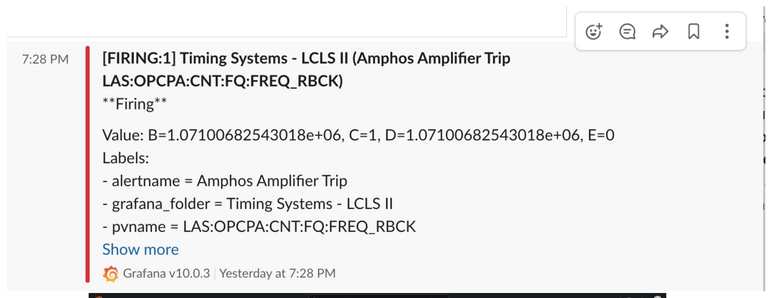
## SOURCES

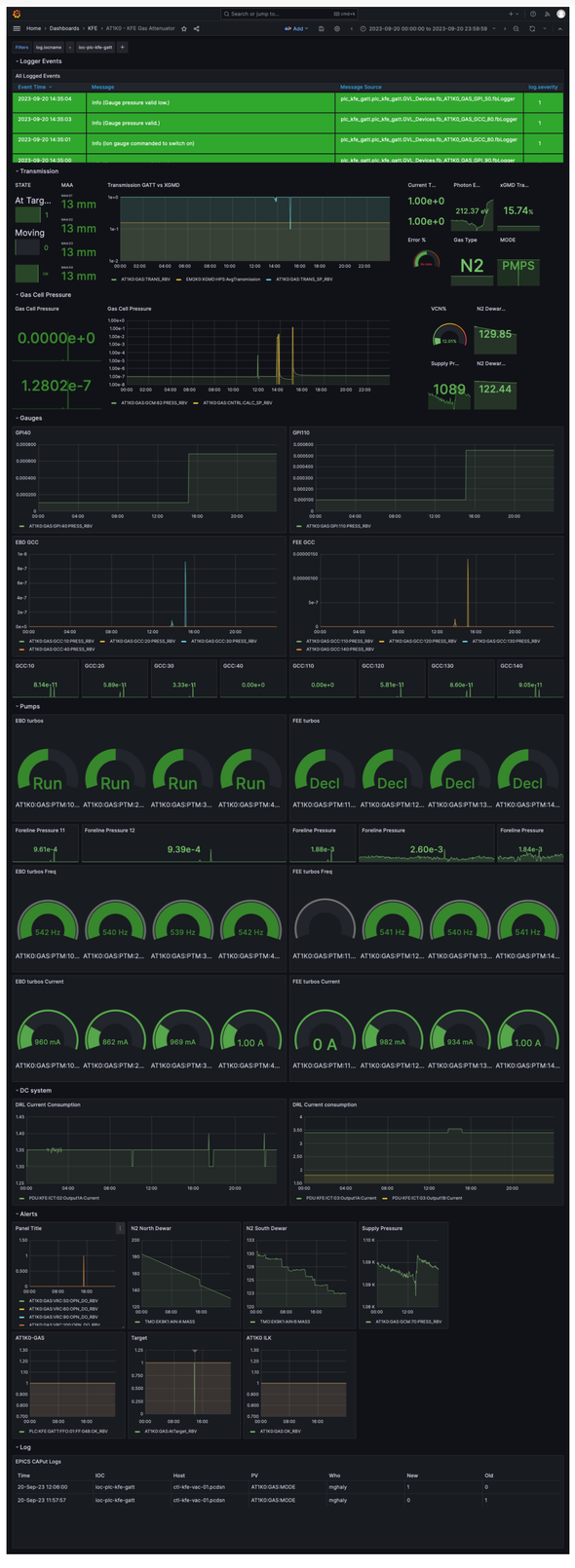
Our centralized logging implementation routes messages from our most common sources to a Logstash instance which is configured to interpret each message and store the parsed information into an Elasticsearch database.

Aggregated logs from all sources can be readily queried alongside historical EPICS Process Variable data [3] in Grafana.


## ALERTING

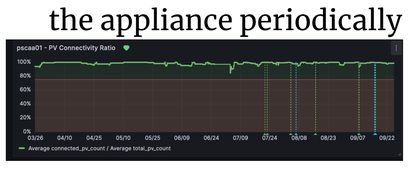
Alerts can be easily configured by end-users to notify users of situations by way of Slack message and e-mail. Below is a sample Slack channel alert that was fired when a value exceeded a threshold.



## ARCHIVER APPLIANCE STATISTICS

As most important EPICS Process Variables (PVs) have been added to the Archiver Appliance for periodic archival, the appliance statistics can be used as a representation of the control system health. An archstats IOC (Python, caproto) queries the appliance periodically for that information.





## PATH FORWARD

This initial deployment has served our team well for the past 3 years, but changes are on the way. We are looking to extend beyond the experimental side of the LCLS: a collaborative effort with the accelerator will yield an LCLS-wide logging system based on Promtail and Loki. Pre-filtering and JSONification of raw, unfiltered EPICS logs is also under consideration.

## ACKNOWLEDGMENTS

SLAC National Accelerator Laboratory is operated by Stanford University for the U.S. Department of Energy Office of Science. Work supported by U.S. D.O.E. Contract DE-AC02-76SF00515

1. Logstash configuration for all data sources: https://github.com/pcdshub/pcds-logstash
2. Archstats IOC for Archiver Appliance statistics: https://github.com/pcdshub/archstats/
3. Shinya Sasaki's Archiver Appliance Grafana data source: https://github.com/sasaki77/archiverappliance-datasource