CONTROL SYSTEM INFRASTRUCTURE
SAFETY SYSTEM

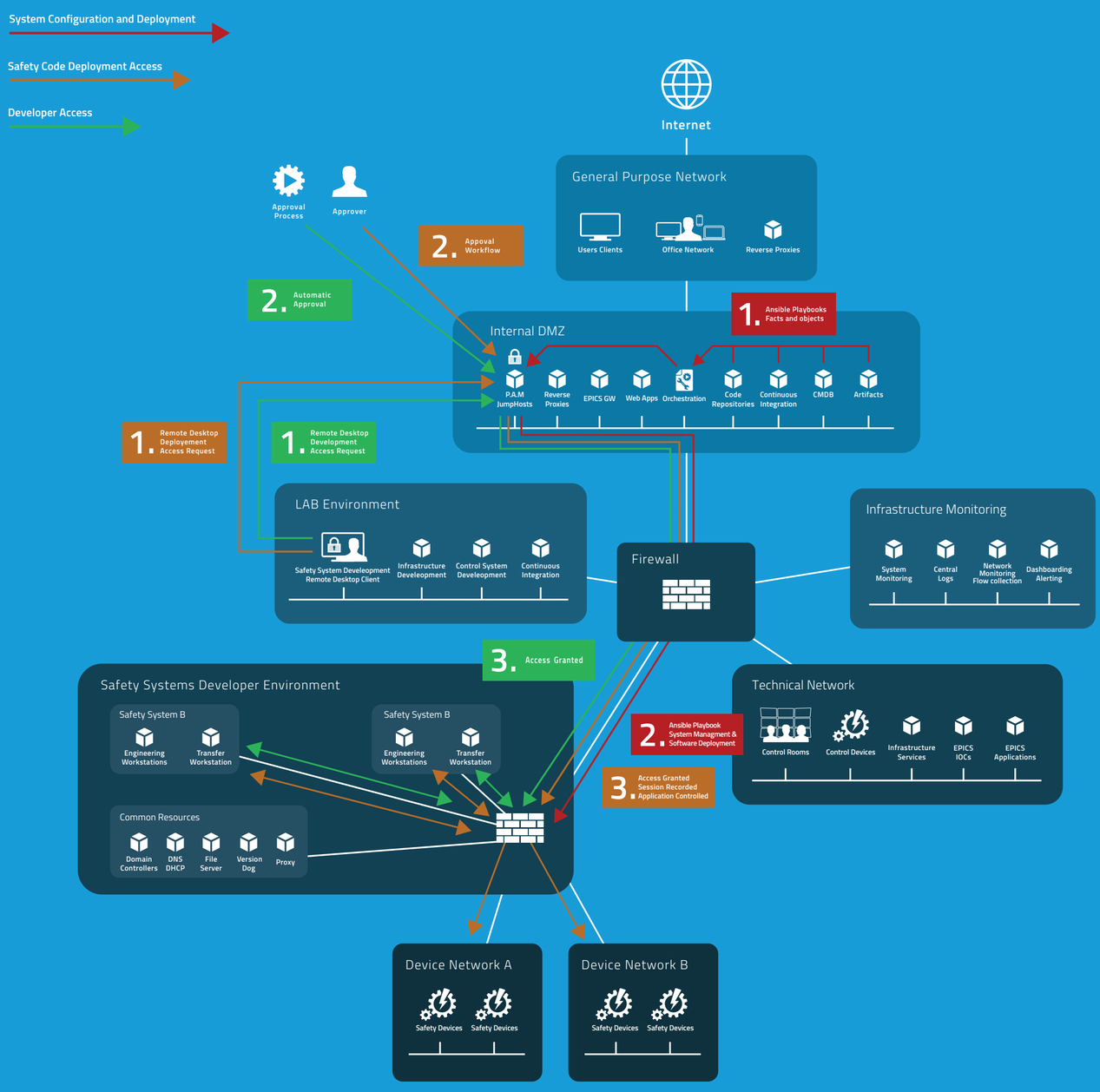
Stephane Armanet, ESS Lund Sweden, October 7, 2019

Abstract

The Control System Infrastructure team has deployed a dedicated isolated environment to support Safety Systems development at ESS. We have tried to take advantage of our standardised infrastructure components for cotrols like virtualization, centralized storage, system orchestration and software deployment strategy. Because we already have all these components in place for our Control System IT infrastructure we have decided to treat engineering workstations as disposable components in an isolated and dedicated virtualized environment.

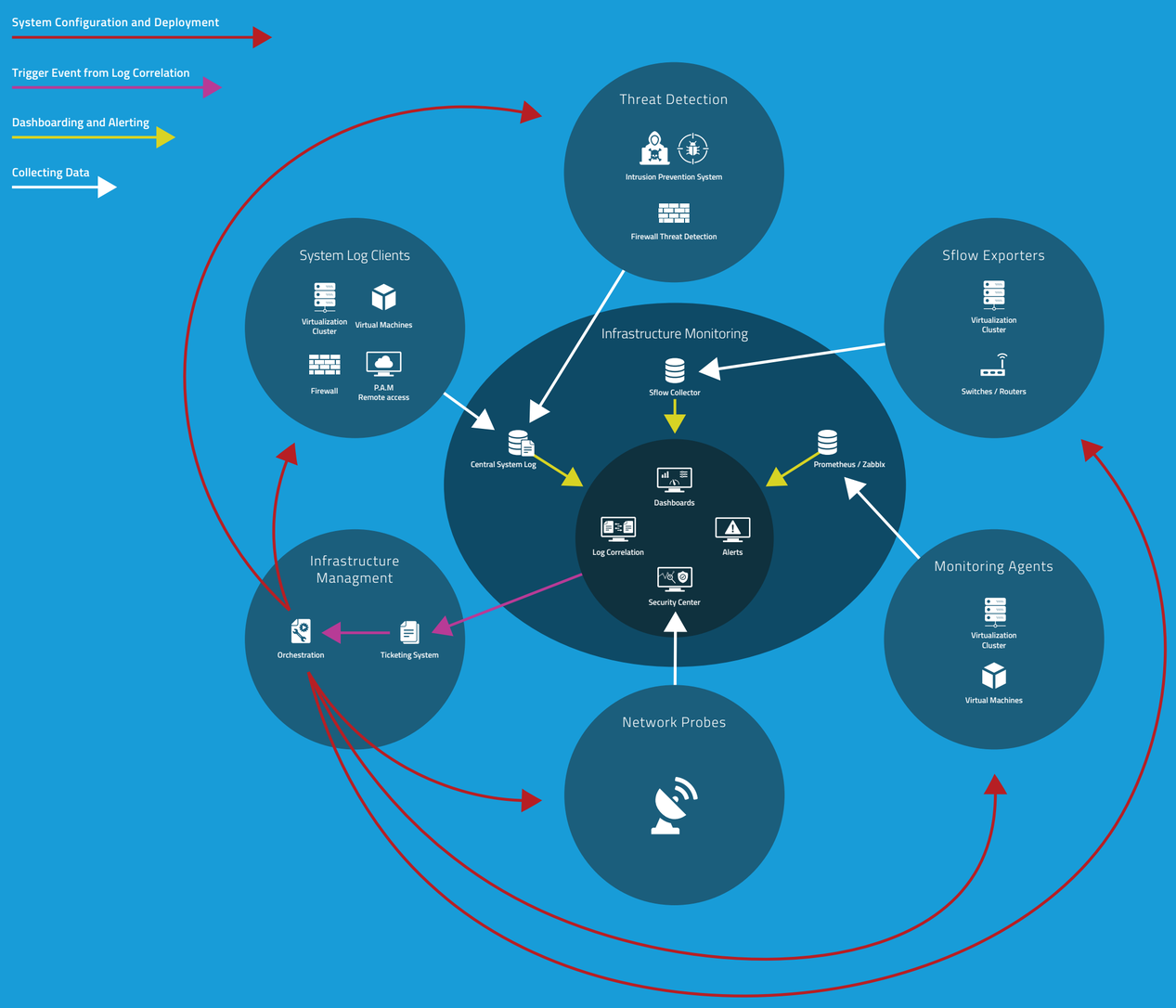
We have designed the environment to control who and when users can access the development environment, from which device, to which workstations and what they can run in this environment.

Safety System Development Environment



- **Isolated Virtual Environment**
- **Approval Work Flow**
  - Access and Session Control
  - Privileged Access Management
- **End-to-end access control**
  - User Device
  - Engineering Workstation
  - Code Deployment
- **Automated deployment**
  - Orchestration
  - Infrastructure as a Code
  - Central Software Repository
- **Flexible Environment**
  - Different Policies for Different Safety Systems
- **Shared Resources**

Threat Prevention



- **Log Centralisation**
  - Syslog-ng Archiving
  - Graylog
  - Indexation
  - Alerts
  - Correlation
- **System Monitoring: Zabbix and Prometheus**
- **Threat Detection**
  - Next-Gen firewalls
  - Suricata IPS
  - Priviledged Access Management
- **Sflow: network devices and Virtualization Clusters**
- **Dashboarding and alerting**
  - Grafana
  - Elastiflow
  - Alerts (e-mail, Web, Slack)
- **Network Probes and Security Centre**
  - Open Cyber-Security related Tickets
  - Link to Orchestration = Patching & Countermeasure

FEEL FREE TO CONTACT
STEPHANE.ARMANET@ESSS.SE