SLAC Initiatives on

Accelerator Cyber Security

Greg White,
Prepared for EPICS Collaboration Meeting Spring 2023
April 26, 2023

Greg White, for Erwin Lopez, Mark McCullough, Amedeo Perazzo, Ken Brobeck, Mark Foster, Daron Chabot,
Mike Zelazny, Lance Nakata, Matt Gibbs, Andrea Chan, Arash Alavi, Poonam Pandi, Lisa Christiansen, Uy Chu, Syed Hasan

Many Thanks to David Manz (PNNL), Jozsef Gacsal (SecurityLit), Jason Carter (ORNL), Ralph Lange (ITER),
Bob Dalesio, Michael Davidsaver (Osprey DCS), George McIntyre (Level-N Ltd)

U.S. DEPARTMENT OF ENERGY
Office of Science

SLAC NATIONAL ACCELERATOR LABORATORY

Contents

SLAC

1. Accelerator computing
2. Example Cyber Statistics, Regulations, and Thinking

3. Typical Cyber Computer Architecture for Accelerators
4. Conducting a Cyber Security Review

5. Extant Accelerator Control System Cyber Issue, EPICS
6. Improving EPICS cyber security

7. New Cyber Regulatory Framework, Compliance Challenge, and Future

8. Summary

Accelerator Computing

- User facing computers. Unix/Linux, Windows, Apple OS, etc
- Control System Software Framework – commonly EPICS DOE labs
- Fast network, typically Ethernet (10 Gb/s), some proprietary
- Front End computing (Input Output Controllers - IOCs)
- Field Buses (VME, CAMAC)
- FPGA, PLC, programmed logic.

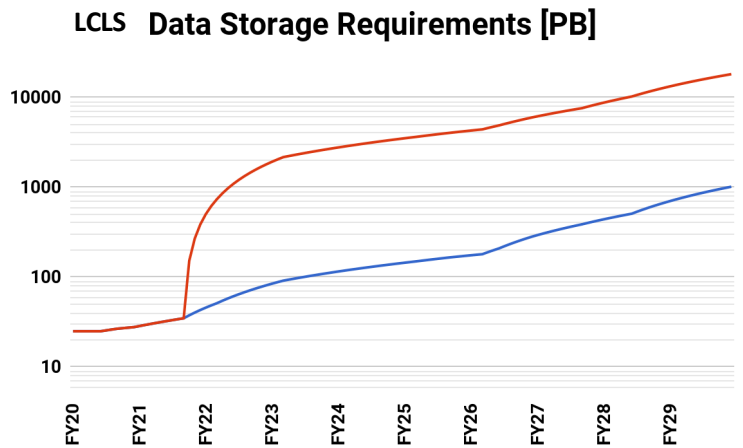
- Display managers (User interface to process variable values)
- High level support software; Matlab, Python, C/C++
- Beam diagnostics, analysis, and beam optimization (High Level) Applications (HLAs)
- Beam Modelling and simulation, High Performance Computing
- Machine Learning (multi-parametric analysis and heuristic reasoning)

Many users, some only peripherally associated with the laboratory. Many kinds of computers, many kinds of network, many tools. Some developed in the community without security oversight, some brought in from outside.

Challenges in Accelerator Computing, Implications for Cyber Security

SLAC

1. Accelerator data and detector data sizes and rates -> Data centers
2. Machine Learning, large-scale optimization -> HPC and Data Center is in production
3. Continuous, online multi-particle modeling -> HPC in production
4. More software for more sophisticated machines -> Vulnerability scanning in prod
5. Machine security. New boundaries in beam power and intensity. *Accidental damage*
6. Cyber Security of large US national assets. *Malevolent Damage*.



	LCLS-II Baseline			LCLS-II-HE		
Dump Unit	E_{max} [GeV]	P_{max} [kW]	<P> [kW]	E_{max} [GeV]	P_{max} [kW]	<P> [kW]
DUMPBSY	4.5	250	90.0	8.0	250	45.2
DUMP2BSY	-	-	-	4.0	125	39.8
DUMP	4.5	120	47.8	8.0	240	56.5
DUMPB	4.5	120	27.0	8.0	120	56.5

Cyber Threat Statistics and Context

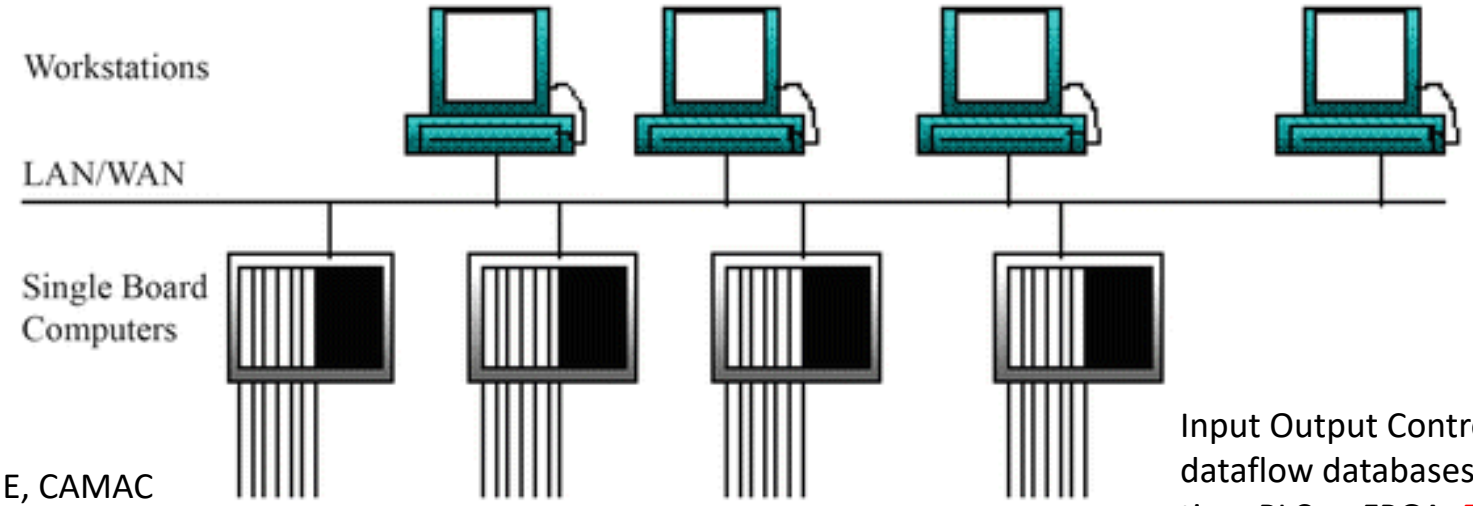
SLAC CYBER EVENT DATA	Q4 2022	Q2 2023
Perimeter defenses stopped attempts. Scanning for known vulnerabilities. Like ssh user brute force attack, Apache path traversal, ZeroShell command execution, etc. Or actual exploits. Like Remote Code Execution (RCE), SQL injection, etc.	33,149,555	509,750,086 (yes 509 M)
Endpoint protection events stopped: Crowdstrike. Malicious software detected. Successfully mitigated by Endpoint protection and response	130	490
Control system intrusions known	0	0
Front-end intrusions known	0	0

Context and thinking

- Historically, accelerator control systems have not included strong cyber security within the network
- We have relied on “secure–perimeter” (sometimes called sequestered network, or “walled garden”)
- The world is a different place
- Is secure-perimeter still advisable? Cf Executive Order (EO) 14028, *Improving the Nation’s Cybersecurity* and *Zero Trust Architecture (ZTA)* and DOE SC orders
- Is EPICS secure? See later in talk.

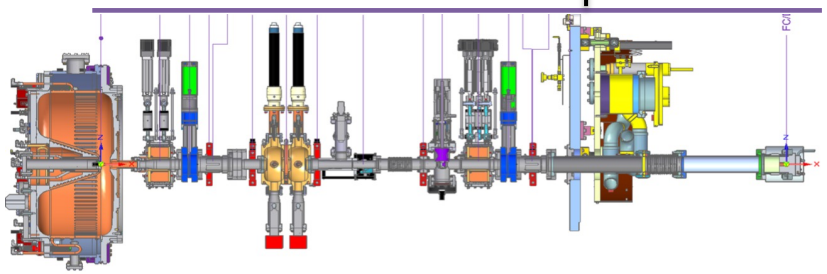
Contents

Distributed Control System + EPICS Cyber Schematic



Control Network. EPICS (CA and/or PVA) in most DOE labs. Others include ACNET, TANGO, SLCMSG etc. EPICS has *Authorization* but no intrinsic *Authentication*.
⇒ Server can't be sure who made a control request. Client can't be sure data came from a given device.

Field Buses;
Allen-Bradley, VME, CAMAC



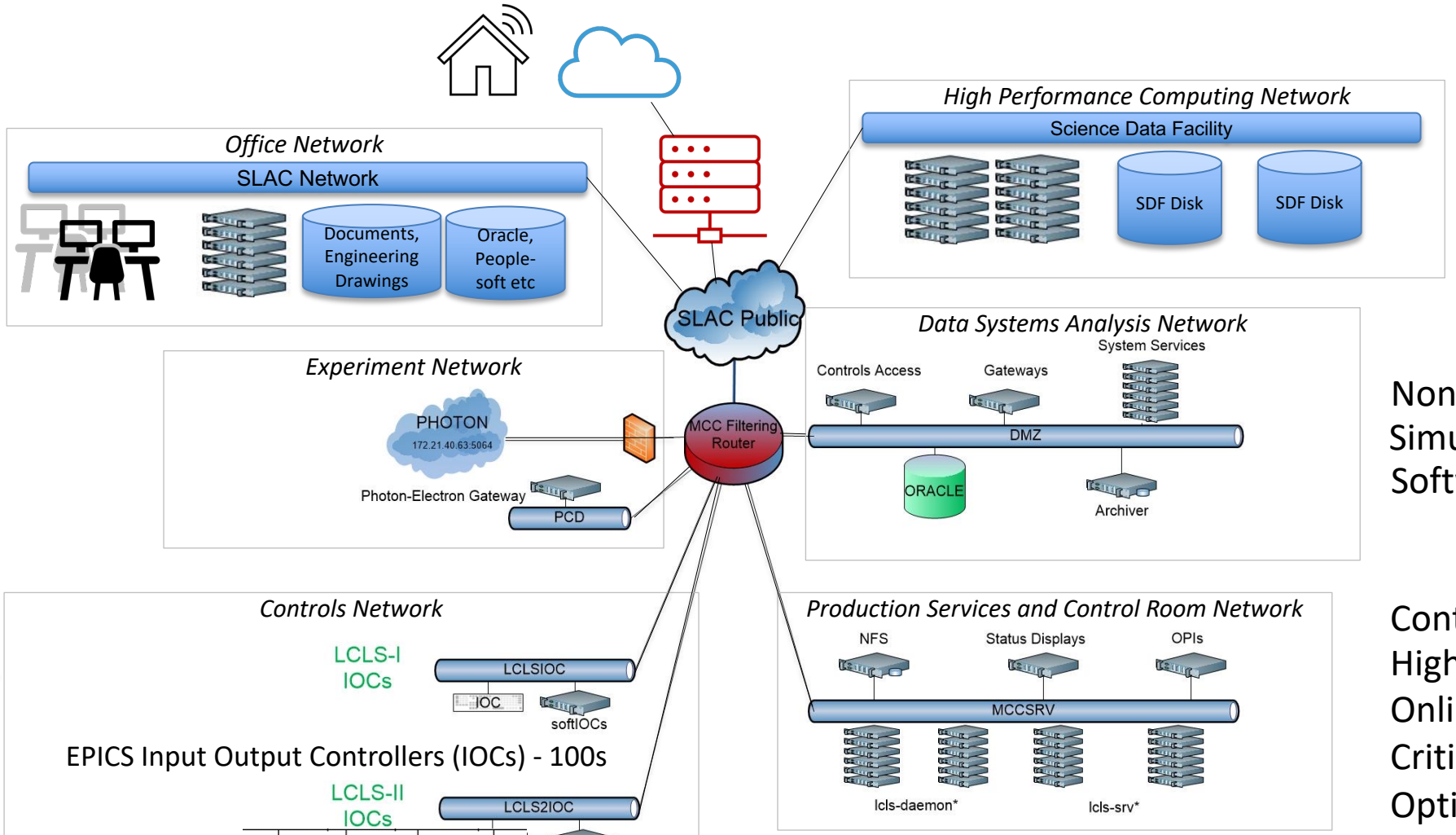
Input Output Controllers (IOCs). Pseudo real-time dataflow databases and device drivers, maybe also real-time PLC or FPGA. Essentially no authentication nor *authorization*. No software signing.
⇒ Can't be sure the computer code you think is running your accelerator is in fact running your accelerator.

Glossary. "AAA":
Authentication: Establish you are who you say you are
Authorization: What set of things are you allowed to do once authenticated
Audit: Keeping track of what you did.

Figure: Simplest Schematic of an Accelerator Control System Network. Computers users, for instance in the control room, connect over a fast network (Gb/s) to front end computers. Those computers in turn connect by field buses and cabling to accelerator hardware for particle generation, beam condition and guidance (electro-magnets), acceleration (RF), diagnostics (beam position), human and machine protection systems, vacuum, cooling etc.

Borrowing from M. Thuot 1996.

Typical Accelerator Computing Architecture (LCLS complex at SLAC)



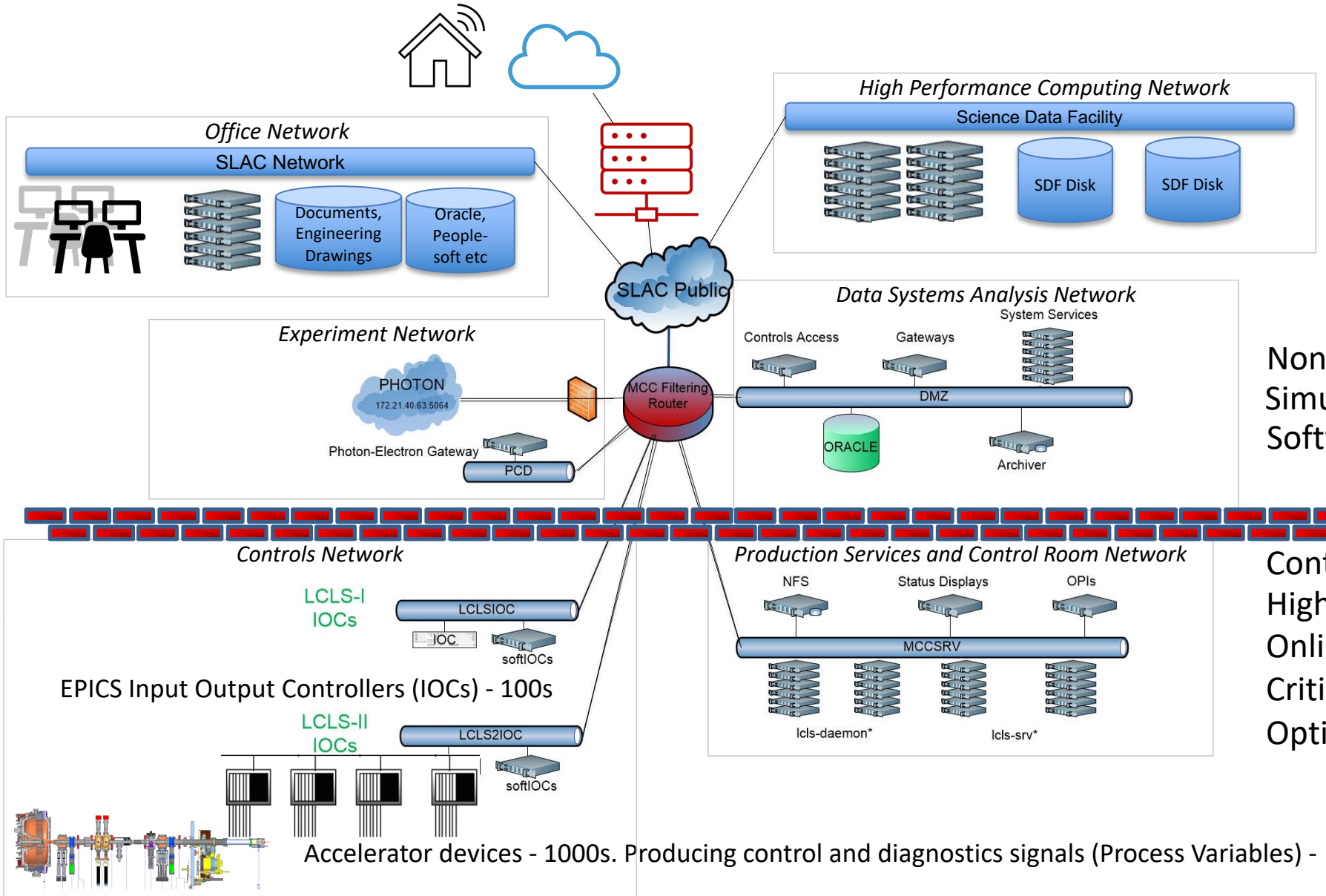
Big Data stores
Experiment Data Analysis
Accelerator Physics Analysis
Multi-particle Tracking (s-2-e)
Machine Learning Training

Non-critical Data Services
Simulation
Software development

Control room displays
High Level Apps execution
Online modeling
Critical Data Services
Optimization, ML and slow feedback

Accelerator devices - 1000s. Producing control and diagnostics signals (Process Variables) - > 8 million at LCLS

Typical Accelerator Computing Architecture (LCLS complex at SLAC)



Big Data stores
Experiment Data Analysis
Accelerator Physics Analysis
Multi-particle Tracking (s-2-e)
Machine Learning Training

Non-critical Data Services
Simulation
Software development

Control room displays
High Level Apps execution
Online modeling
Critical Data Services
Optimization, ML and slow feedback

Accelerator devices - 1000s. Producing control and diagnostics signals (Process Variables) - > 8 million at LCLS

EPICS Authorization. Access Control File (ACF)

```
[physics@lcls-srv01 .../epics/iocCommon/facility]$ more access_security_cryo.acf
UAG(CRYO) { dianek, smcqueen, rredford, vivienl, eidle, kdouglas, gclooney, cryoegr }
UAG(SYSMAN) { sysman }

HAG(CRYOMCR) { cryo-opi01, cryo-opi02, cryo-opi03, cryo-opi04, cryo-opi05 }
HAG(ACR) { opi10, opi11, opi12, opi13, opi14, opi15, opi16, opi17, opi20, opi21, opi22, opi23, opi24, opi25, opi26,
opi30, opi31, op
i32, opi33, opi34, opi35, opi40, opi41, opi42, opi43, opi44, opi45, opi46, opi47 }

ASG(CRYO) {
    INPA(ZIOC:CP00:CR01:CRYO_ACCESS) # Subsystem-specific permissions bit
    RULE(1, READ)
    RULE(1, WRITE) { UAG(SYSMAN) }
    # Global permissions ("CRYO only")
    RULE(1, WRITE, TRAPWRITE) {
        HAG(CRYOMCR)
    }
    # Subsystem Specialist access
    RULE(1, WRITE, TRAPWRITE) {
        CALC("A=1")
        UAG(CRYO)
        HAG(SRV)
    }
}
```

*Example: Access Control File for LCLS Cryogenic Systems, showing individual **user names**, **computer names**, that the cryo control room can write a cryo PV at any time, and that cryo specialists can write to a cryo PV only if they have been enabled to do so by operations.*

Experience of SLAC Accelerator Cyber Assessment
1. Scope and Objective

SLAC

System Experts charged with assessment of resilience to cyber attack on:

1. Operations (for instance deletion of required software)
2. Physical accelerator controls (e.g. malicious write to PVs of cryo facility)
3. Accelerator configuration basis (e.g. magnet polynomials in Oracle)
4. Data, analysis or diagnostics (e.g. deletion or change of archived values).

PPS cyber security was not investigated. We did NOT consider physical security such as vacuum of cryomodule, cavity tune, etc.

Results used to plan immediate improvements and further analysis. Experts directed to highlight items that worried them. And to use the systems analysis to investigate and propose fixes.

Experience of SLAC Accelerator Cyber Assessment cont'd

2. Systems in Scope

SLAC

1. SLAC IT Network; routers, gateways, Domain Name Services.
2. Control System Access mechanism:
   Enterprise (SLAC) Identity Access Management -> DMZ bastion -> ssh public key
3. Accelerator Control System Hosts
4. Control System Software security
   a. PV write authorization security (EPICS Channel Access - "ACLs" for PVs)
   b. Control Protocol security (EPICS Channel Access, PvAccess)
   c. Front end computer security (EPICS IOC software, FPGA, field busses etc)
   d. Beam diagnostics, tuning and optimization security (Matlab, Python)
5. Data Stores: EPICS Archiver, High Performance timeseries data stores
6. Intellectual Property Stores: Physics Log, Operations Log
7. Databases: Oracle (Device Infrastructure, Magnet, Cabling, Issue management, etc)
8. High Performance Computing Systems
9. Controlled Document store (Sharepoint)
10. Engineering Drawings (Windchill, Solid Edge, AutoCAD, SODA)

Experience of SLAC Accelerator Cyber Assessment cont'd
3. Systems Specialists Briefing & Response Template

For each system assignment:

- Describe the use of the system in brief
- Describe existing security measures, assess any weaknesses, and highlight missing coverage
- Tabulate the system with respect to the following. For each defense type, if the system includes it, describe the defense's implementation in the system. If the defense is not pertinent to the system, enter "N/A". If the defense would be pertinent to the system, but is not in fact employed, enter "Not implemented" and, if possible, details of what you would recommend.

Security or Cyber Defense Type	Describe
Authentication, Authorization, Audit. Kerberos, SSL public/private key	How is a user authenticated to the system. Is Authentication for instance by Kerberos? How are communications encrypted (if at all)
Known Vulnerability scanning	Is the system scanned for known ways to hack?
Backups	Verify backups exist and are being updated. Document the backup schedule and where backups are located. Are backups secure against system failure, power, fire.
Malware Detection	Is the system included in Crowdstrike?
Accelerator self-defense – EPICS LO/HI limits, MPS, BCS	For accelerator controls, what mechanisms exist to ensure proper operating range?
Air-gapped processor-observer pattern (as in PPS)	Does any part of the system include air-gapped or one-way only communications (data diode) security?
Network segmentation	Is the system hosted in a controlled or otherwise confined network?

Findings of SLAC Accelerator Cyber Review

System	Authentication Authorization and Audit	Vulnerability Scanning	Malware Det. (Crowdstrike)	Backups	Accelerator Protection system	Air-gap / process-observer	Network Segmentation
MCC. Accelerator Controls Networks - ~OSI 7 Layer Model levels 1-5	ssh rsa/dsa public-private key using SLAC User ID and mcdogin as a bastion host. VMS password.	No vulnerability scanning on accelerator networks, for fear of interference with ops. Yes, at DMZ level.	No malware scanning on accelerator networks, for fear of interference with ops. Yes, at DMZ level.	Yes. All NFS data and systems are backed up by coordination with OCIO. Operational to MCC (bldg. 5). Disaster recovery to ANR (B52). Large data to AFS.	N/A	No. Direct authenticated login is supported.	Yes. Filtering Router enforces DMZ intermediates SLAC to prod. Each accelerator network is segmented into a few functional VLANs.
EPICS. Accelerator Controls Networks ~OSI 7 Layer Model levels 6-7	No control network user Authentication. EPICS PV change Authorization being added.	No. IOC processes and client servers are not scanned for vulnerabilities.	No. No malware detection of EPICS processes on Production . No front end executable certification	Access Control Files backed up by virtue of AFS.	Yes, extensive but may be incomplete. Facilitated by EPICS DRV-L/H, MPS, BCS.	Not as such, but separation mediated by router is sometimes used.	Yes. Production networks are isolated via DMZ.
SLAC Science Data Facility (aka S3DF)	Kerberos (until SLAC standard federated is available)	Yes. S3DF DMZ daily. Others biannual.	Yes - DMZ & Workstations. No - HPC and core.	Yes (as of Aug 22).	N/A	Not employed. S3DF is intended for access internally and externally.	Yes.
SLAC Enterprise Networks (SLAC IT)	Networking device management requires authentication by Kerberos + DOE PIV card.	Yes, admin. by SLAC cyber.	Yes. Networking management hosts have CrowdStrike. Devices (routers etc) do not.	Yes. Backups daily to SLAC AFS and Stanford AFS.	N/A	No. SLAC IT does not operate any air-gapped enterprise networking	Yes. SLAC Networks are segmented; access and firewall implemented individually for each.
Oracle & APEX.	UserID + Oracle db pwd or Oracle wallet. LDAP & WebAuth for APEX.	Yes, admin. by SLAC cyber.	Yes on main SLACPROD dbs. No on MCCO dbs.	Yes. Full and incremental backups daily. 30 day retention.	N/A	No.	DBs segmented by content. Diff. pwd/wallet required for each. MCCO is in DMZ.
Controlled Document Management System (CDMS)	SLAC Active Directory & MFA. MS has no access to SLAC cloud data.	Yes, admin. by MS.	Yes, administered by MS.	Yes, redundancy and resiliency by MS. We assume their diligence	Content describes Accelerator Protection Systems.	No.	Yes [2]
Engineering Drawings and Data (TC / SEDA)	TC req SLAC ID of named license holder. SEDA req SLAC ID/ MFA	Yes, admin. by SLAC cyber.	Yes, admin by SLAC cyber.	TC: Yes, admin by SLAC IT. SEDA: Yes, admin by MS.	N/A	No.	Per TC system.
High Level Applications (HLA)	Presently, all HLAs are on prod, so AAA is per MCC and EPICS above.	No, not in production.	No, not in production.	Yes, per MCC.	Partly. Mostly rely on EPICS limits.	No. However do have read-only gateway.	Yes, per MCC.

Figure: Example table of cyber review findings, showing each of 8 system's cyber situation on 7 metrics

SLAC

SLAC Summary: Positive Overall. Our cyber security was found complete with respect to common practice.

1. Login security is comparable to most facilities. Will soon be leading
2. Backups are complete
3. Malware Detection & Vulnerability Detection are complete (subject to the norm that malware detection is not run in production)
4. CA Security (authorization to change PV) is designed, in cryo IOCS, and ready for broad implementation

All EPICS Labs

However, EPICS itself is insecure. Its use is based on aging assumption of secure perimeter. Lacks strong authentication and software signing.

Contents

EPICS Controls Security Issues & Recommendations

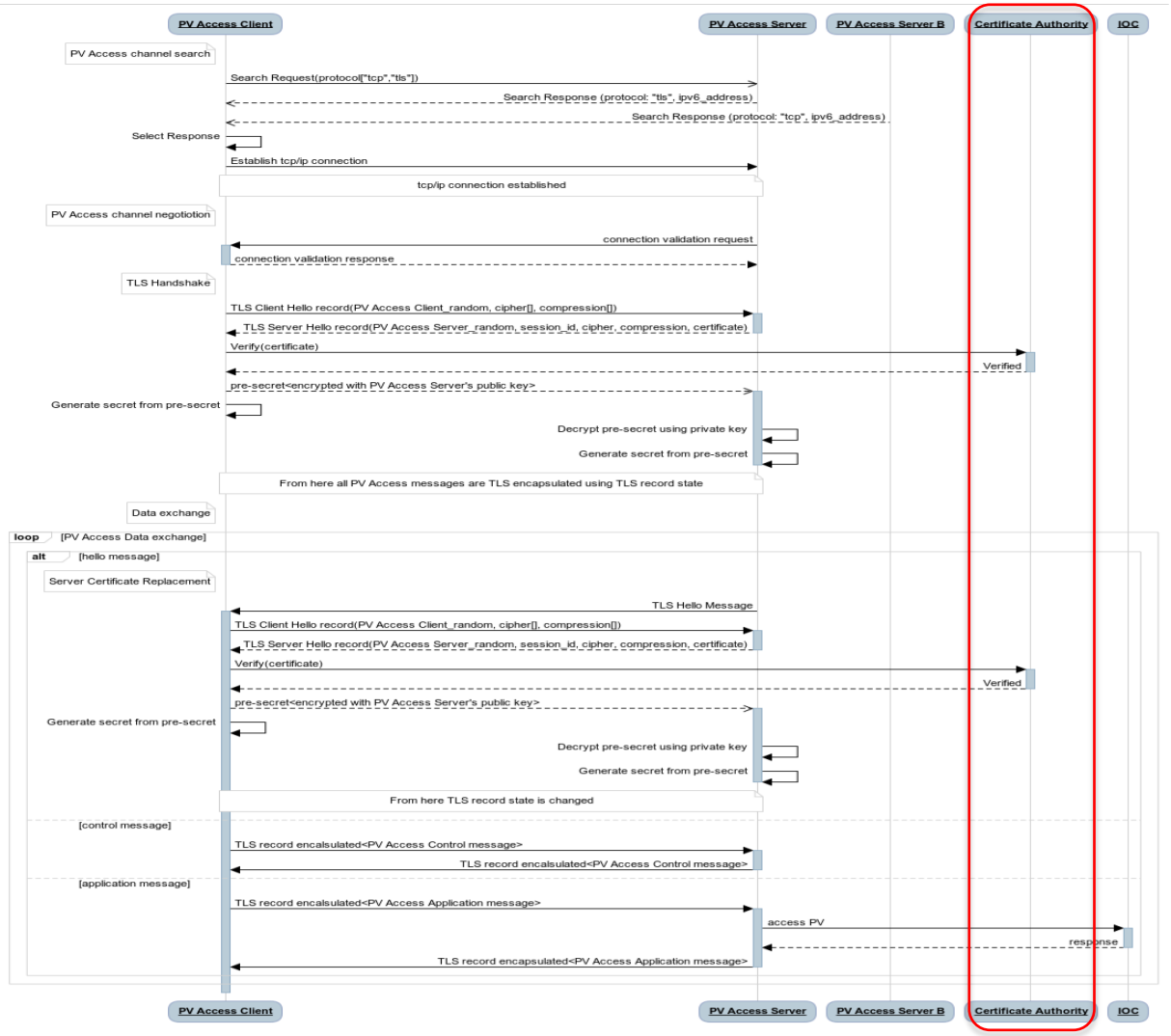
SLAC

- **Passive Traffic Inspection**
  Passive attacker can observe and learn Process Variable and server names. Not considered serious.
  ⇒ Could Mitigate by TCP+TLS(*)
- **PV Denial of Service by search spam**
  Active attacker responds to PV search requests, directing to null server
- **PV Search Hijacking / Man in the Middle Attack**
  Active attacker responds quickly to all observed searches, redirect clients to rogue EPICS server.
  Returns fake data, or proxy forwards bad control data to a legitimate control system EPICS server.
  Very bad things.
  ⇒ Mitigate by adding Transport Layer Security (as long as attacker does not hold certificate)
- **Server impersonation / credential theft**
  Theft of server certificate used to maliciously impersonate PVs provided a legitimate server.
  ⇒ Mitigate by something like certificate "pinning."

(*) Transport Layer Security (TLS); Encryption, certificate-based authentication, compression.

Work of Michael Davidsaver, Osprey DCS, under SLAC contract, 2021

EPICS Security Improvement: PvAccess and Transport Layer Security (TLS)



- PvAccess + TLS = First step to Zero Trust Architecture in EPICS Accelerator controls
- Multi phase project:
  - Server side authentication
  - Client side
  - Certificate server? Name Server? Pinning?
- Transition phase: EPICS pvAaccess TLS would be fully backward compatible. TLS aware endpoints co-exist with non TLS.
- Goal: All endpoints use PvAccess + TLS. NOTE security implies removal of legacy Channel Access protocol from EPICS systems (!)

Figure: EPICS PVA negotiation with TLS proposal, showing:
TLS handshake after message validation,
"tls" message, cipher handshake, and certificate verification additions to EPICS PvAccess protocol.
Modification uses the "magic" byte in the pvAccess header, and existing protocols field in the search response.

Work of George McIntyre, Level-N Ltd, + Michael Davidsaver, Bob Dalesio, Osprey DCS, under SLAC contract, 2022

Contents

SLAC

Cyber Security Regulatory Framework

- Executive Order (EO) 14028, *Improving the Nation's Cybersecurity.* Calls for a "Zero Trust" posture
  - OMB Memorandum M-22-09*, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
    - DOE Plan to Implement Zero Trust Architecture (ZTA), July 11, 2021
    - DOE Improving Cybersecurity: Guide to Implement Zero Trust Architecture, DOE OCIO, March 2022
    - DOE Moving the U.S. Government Toward Zero Trust Cybersecurity Principles Zero Trust Strategy Document. M-22-09, Gina Fisk, DOE-SC CISO, July 2022

DOE Zero Trust Order Compliance Gap Analysis

Zero Trust Architecture order [2] Principle; authenticate individuals for each action they take; and make authentication so ubiquitous that the secure perimeter can and should be dismantled.

DOE Zero Trust Guidance (from [6])	Norms in Accelerator Distributed Controls network
Assume no implicit trust is granted to users, … or resources.	A lot of implicit trust granted to accelerator users
Foundational tenet… no resource is inherently trusted	Resources frequently trusted. No way to verify identity nor true operation of resource. EPICS+TLS would enable resource certification.
… and must be continuously authenticated	Rarely re-authenticate. Could add. Implies work disruption
Encrypt data-at-rest and data-in-transit	Control data-in-transit not encrypted. EPICS+TLS would enable encryption. Data-at-rest (stored, archived) not encrypted. Could add, though won't be popular.
Multi-factor authentication	MFA rare inside controls. Possible to add MFA to ssh. Must consider MFA for operations.
Malware Detection everywhere	Uncommon for malware detection in high performance, high availability control systems. Rare for malware in front end computing.

Contents

SLAC

Plan for SLAC Accelerator Cyber Security

Pursue:

- Complete Channel Access Security
  - Individual Logins. Negotiate on OPI logins. Think through implication of common id on OPIs for EPICS attacks
  - Deploy ACL files
- Penetration Test. Multi-phase - outside SLAC to SLAC, from inside SLAC to control, stealth, non-stealth etc.
- EPICS PVA+TLS
  - Server side first, then client
  - CA will have to be removed.
- SSH with MFA
- MAC registration
- Malware detection (CrowdStrike) in Accelerator Network assessment
- Vulnerability detection in Accelerator Network assessment
- Collaboration and Partnership with EPICS community.

Negotiate / seek exemption from Office of Science on ZTA:

- Encryption at rest. Cf Stanford Research Policy Handbook (RPH), section 1.4, Openness in Research
- Re-authentication. Too disruptive to operations.

Penetration Test Experience

SLAC

Method:

- Safety Critical Systems addresses removed
- Other production included (while machine was down)
- Developers on dev networks (!) working on kinetic or high voltage systems need formal warning
- Formal table of addresses whose pen test is controlled. Other addresses included

Pen Test Conclusions:

- Pretty good.
- For future pen testing - “canary traps” for port scans in important networks
  - Developer safety (!). May have to control pen tests as a safety matter! Like LOTO.
  - Critical systems (PPS, BCS etc)

Summary

SLAC

1. Accelerator Computing involves many interconnected systems
2. Distributed control often relies on a sequestered network architecture and assumption of security within the network
3. The world is different, and we must adapt
4. Recent EO, OMB and DOE regulations require serious thought about assumptions
5. True Accelerator Cyber Security will be a long hard challenge
   - We've started on the road with EPICS PvAccess + TLS
   - Many challenges remain, particularly legacy systems ubiquity.
6. External Consultancy for penetration testing accelerator
7. Is port scanning a safety hazard that must be safety controlled (PJB, LOTO etc)?
8. DOE can help with clarification, funding and materially supporting collaboration toward a nominal architecture for controls and experimental systems cyber security.

References

1. Cybersecurity Capability Maturity Model (C2M2), June 2019, DOE, https://apps.dtic.mil/sti/pdfs/AD1078768.pdf
2. Executive Order (EO) 14028, *Improving the Nation's Cybersecurity,* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ Calls for a "Zero Trust" posture
3. OMB Memorandum M-22-09*, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
4. DOE Plan to Implement Zero Trust Architecture (ZTA), July 11, 2021
5. DOE Improving Cybersecurity: Guide to Implement Zero Trust Architecture, DOE OCIO, March 2022
6. DOE Moving the U.S. Government Toward Zero Trust Cybersecurity Principles Zero Trust Strategy Document, Gina Fisk, DOE-SC CISO, July 2022

BACKUPS

SLAC ACCELERATOR CYBER REVIEW FINDINGS

SLAC

Positive Overall. Our cyber security is complete with respect to common practice.

1. Login security is comparable to most facilities. Will soon be leading
2. Backups are complete
3. Malware Detection (Crowdstrike) & Vulnerability Detection are complete (subject to acceptance of the common principle that the control system be exempt from these).
4. CA Security (authorization to change PV) is designed, in cryo IOCS, and ready for broad implementation

However, EPICS is insecure. Its use is based on aging assumption of secure perimeter.

1. EPICS protocols lack strong authentication
   a. Man in the Middle attack. A PV could be changed without ACR knowledge
   b. EPICS users will be authorized for PV changes, but aren't presently strongly authenticated
2. IOC Software is not certificate authenticated (user can't be sure the IOC they're talking to is not an imposter)

Additionally, some administration and management:

1. PV drive limits are not all set – can lead to machine errors
2. Understaffed with Oracle DB Admin

Argonne (APS) Controls Computing Example

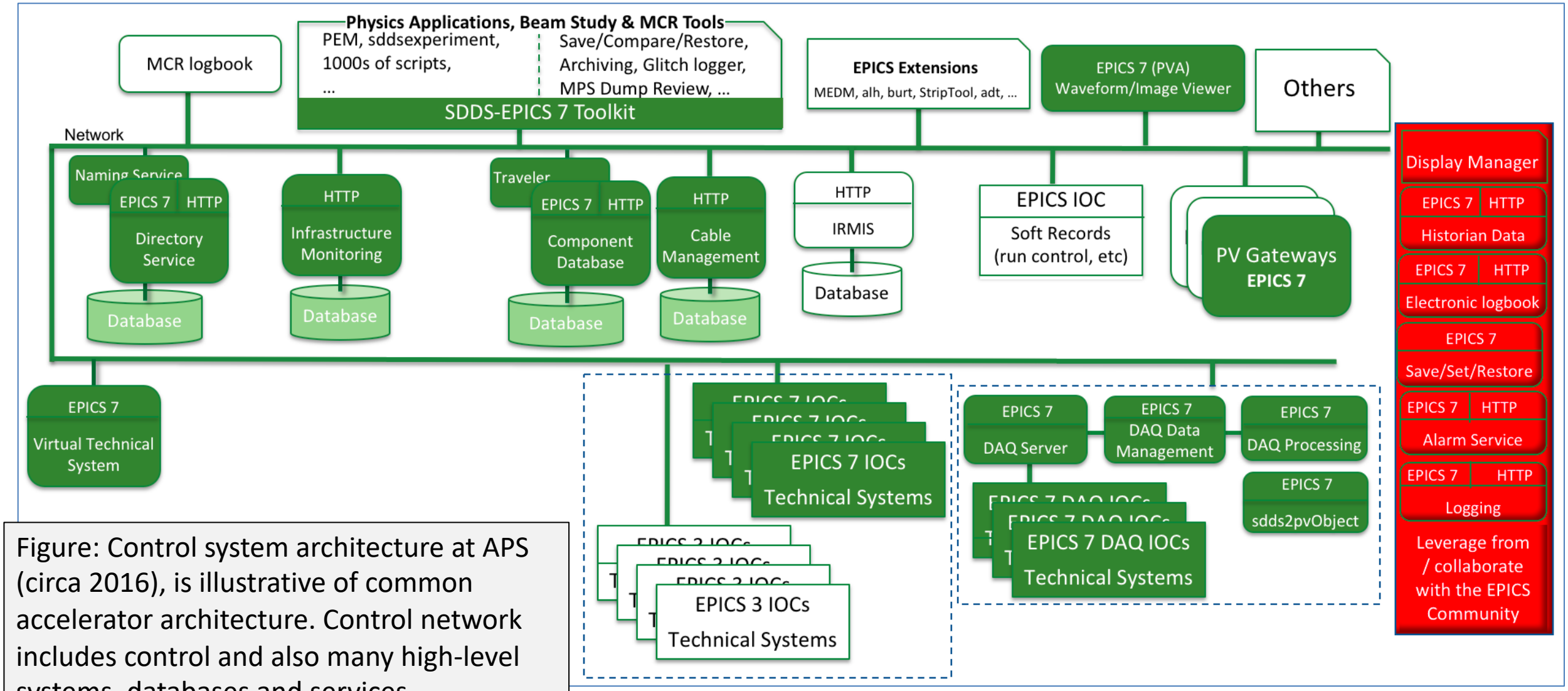


Figure: Control system architecture at APS (circa 2016), is illustrative of common accelerator architecture. Control network includes control and also many high-level systems, databases and services.

Siniša Veseli, Andrew Johnson, Guobao Shen, ANL