



Month Day, Year

ICALEPCS 2025: Managing Technical Debt Across Large- Scale Control Systems

Adam Watts
Senior Engineering Physicist



U.S. DEPARTMENT of ENERGY Fermi National Accelerator Laboratory is managed by FermiForward for the U.S. Department of Energy Office of Science

This manuscript has been authored by FermiForward Discovery Group, LLC under Contract No. 89243024CSC000002 with the U.S. Department of Energy, Office of Science, Office of High Energy Physics.

Who am I?

- Adam Watts, Senior Engineering Physicist at Fermilab.
- Member of Accelerator Directorate, Controls Department.
- Group leader for Industrial Controls.
- Project Engineer for ACORN control system upgrade project.
- Former beamline physicist for 40+ year-old experimental beamlines.



Summary: career so far defined by inheriting significant technical debt.



Technical Debt

Technical debt is the accumulated burden of maintaining short-term solutions that, due to lack of resources, became permanent.



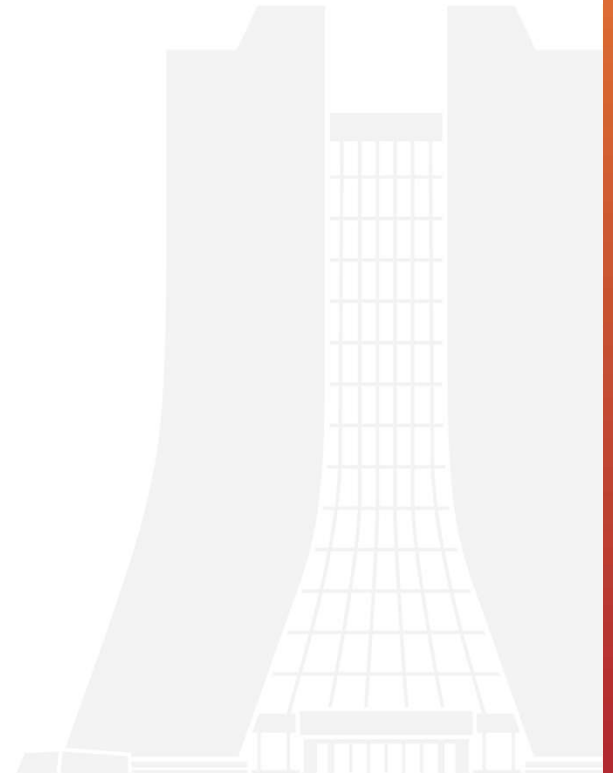


Familiar scenario?

Raise your hand if you inherited a system like this:

Essential to operations.

"That's Dave's Box, and it runs the lab.
Nobody knows how."





Familiar scenario?

Raise your hand if you inherited a system like this:

Essential to operations.

"That's Dave's Box, and it runs the lab.
Nobody knows how."

Critical components are no longer made or supported.

"Dave only used vacuum tubes and COBOL."





Familiar scenario?

Raise your hand if you inherited a system like this:

Essential to operations.

"That's Dave's Box, and it runs the lab.
Nobody knows how."

Critical components are no longer made or supported.

"Dave only used vacuum tubes and COBOL."

Documentation is of poor quality, lost, or non-existent.

"Dave can tell you everything you need to know."



Familiar scenario?

Raise your hand if you inherited a system like this:

Essential to operations.

"That's Dave's Box, and it runs the lab.
Nobody knows how."

Critical components are no longer made or supported.

"Dave only used vacuum tubes and COBOL."

Documentation is of poor quality, lost, or non-existent.

"Dave can tell you everything you need to know."

Single owner/maintainer/designer is no longer available.

"Dave died 10 years ago."

Contributing factors at accelerator labs.

- **Uptime and operational reliability**
 - Control systems don't typically turn off, even during maintenance periods.
 - Constant pressure to return systems to operational state at all costs, as soon as possible.
- **Integration complexity**
 - Large scope of heterogeneous devices and code-bases needed to run accelerators.
 - Control systems interface to legacy equipment/code, or equipment/code implemented by a short-term experiment or graduate student.
- **Staffing model**
 - Engineers, technicians, operators, scientists.
 - Diverse and sometimes competing needs/goals.
 - Heavy matrix management, constant context-switching.



Typical control system architecture diagram.

There are multiple types of technical debt.

- **Design debt**

- Myopic design decisions.
- Example: *hard-coded 15Hz proton source repetition rate at Fermilab.*

- **Documentation debt**

- Systems lacking comprehensive documentation.
- Example: *“Dave may have written things down on a napkin 40 years ago.”*

- **Code debt**

- Software that works, but isn't maintainable.
- Example: *“It compiles, so that means it must work!”*

- **Infrastructure Debt**

- Dependencies on obsolete hardware, locked-in to vendor ecosystems, unmanaged library dependency chains.
- Example: *COBOL and vacuum tubes.*

- **Process Debt**

- Lack of formal change management practices, unclear organizational boundaries, inadequate communication.
- Example: *Orphaned PLC from another group with code that doesn't match the latest documentation.*

How to start digging out of technical debt.

Reactive strategies: now that we're in this situation, what do we do?

- **Risk-Based Lifecycle Management**
 - Track component lifespans and risks, revisiting annually to prioritize upgrades.
 - Plan for obsolescence, develop cost/labor estimates for inevitable upgrades.
- **Cost and labor tracking**
 - Quantify the operational cost of maintaining technical debt systems.
 - Contrast to investment cost of needed upgrades.
 - Consider fault-tracking systems to identify worst offenders.
 - Management buy-in is crucial to allocate resources accordingly.
- **Transparency**
 - Be open and honest about the operational impact.
 - Heroics to keep systems limping along can cover up systemic problems with technical debt.
 - *"The squeaky wheel gets the oil"*: if you need oil, start squeaking.
 - Avoid the instinct to implement further short-term fixes, which compound technical debt.
 - Set stakeholder expectations about reliability and time-to-repair for legacy systems.



How to prevent more technical debt.

Proactive strategies: how to mitigate getting in this situation again?

Documentation and Knowledge Sharing

- Provide a clear “first place to look” for any system: what it does, why it exists, and how decisions were made.
- Documentation is the cheapest insurance against siloed expertise.
- Adopt standard documentation forms to ensure consistent information, ease onboarding and culture change.

Standardization of Implementations

- Consolidate solutions into a manageable set of standard approaches.
- Translate stakeholder needs into supported “buckets”, negotiating when requirements exceed scope.
- Expand buckets only when resources are available to maintain them.

Modularity, Extensibility, Interoperability

- Design cohesive modules with clear responsibilities.
- Favor extensibility to meet future needs, while guarding against scope creep.
- Avoid vendor lock-in by favoring widely-used interfaces and standards.

Disciplined Development

- Prioritize supported solutions over shiny new ones.
- Use prototyping and controlled iteration to validate needs before committing to large builds.

Collaborative Stakeholder Engagement

- Work closely with stakeholders to get on the same page about system requirements.
- Differentiate between required functionality and “nice to have” conveniences.
- Agree on the definition of a minimally-viable product: what is the base functionality to achieve? Treat anything above that as future improvements.
- Use a commissioning/testing/validation procedure to document satisfaction of agreed-upon requirements.
- Set expectations: added scope means more resources (time, labor, money) are needed.
- Agree on a reasonably-estimated schedule. Communicate delays as soon as realized. Stick to the schedule: impatience leads to unnecessary time pressure, which leads to cutting corners.

Example: Collimator motion control

Itemizing requirements from stakeholder specifications, developing relevant testing plans to validate.

Category	Description	Test
Machine Protection	Machine protection beam permit shall be disabled if communication between the PLC and front-end are lost.	Unplug ethernet cable from PLC and observe beam permit dropping.
Readings	Remote readbacks shall occur at a minimum of 20 Hz.	View logged position data to confirm 20 Hz rate.
Readings	The thermocouples shall be capable of reading a maximum of 12000 C.	Verify with thermocouple, conditioner, and ADC specs.
Readings	The jaw position shall be read out at a minimum resolution of 0.25mm.	View logged position data to confirm resolution while making very small slow motor position changes.
Machine Protection	The beam permit shall drop no later than 2 seconds after a jaw position limit is reached.	Used logged data to show interval between exceeding LVDT permit limit and permit drop.
Machine Protection	The control system shall take no longer than 2 seconds to average a thermocouple reading.	Measure PLC scan time when code sequence is finalized.
Readings	Limit switch status shall be remotely viewable via the control system.	Move collimator position from one limit to the other, verify limit switch visibility in control system.
Readings	Thermocouple readings shall be remotely viewable via the control system.	Verify real-time and logged thermocouple readings. Disconnect each to verify the correct parameter reading changes.
Readings	Jaw LVDT readings shall be remotely viewable via the control system.	Verify real-time and logged LVDT readings in control system when moving motors.
Machine Protection	Limit switch failures must present a "fail-safe" scenario that leads the machine protection system beam permit dropping.	Disconnect limit switch from PLC or punch-down panel, verify beam permit drop.

Itemizing requirements from the specifications document the stakeholder provided.

Outer Limit Switch	825VUS	825HUS	825VDS	825HDS	827VUS	827HUS	827VDS	827HDS
Move jaw to OUT limit.								
Verify OUT limit switch disengages motion.								
Verify on a parameter page that the motor step count jaw position readbacks move in the correct direction								
Verify that the datalogged motor step count jaw position readings reflect moving to the OUT limit.								
Verify on a parameter page that the LVDT jaw position readbacks move in the correct direction								
Verify that the datalogged LVDT jaw position readings reflect moving to the OUT limit.								
Verify that there is a control system alarm to show that the LVDT jaw position has exceeded the alarm limit.								
Verify digital status in control system indicates the OUT limit switch engaged. Verify that the machine protection permit changes to a beam disable state when the OUT limit switch is engaged.								

Building test procedures to validate satisfaction for the requirements.



Example: PLC document responsibilities

Setting expectations with stakeholders.

Information/Document	Responsibility	Information/Document	Responsibility
System description	System engineer	PLC bill of materials	Industrial Controls
P&ID	System engineer	Ladder logic repo	Industrial Controls
List of sensors	System engineer	I/O spreadsheet	Industrial Controls
Requirements	System engineer	Wiring spreadsheet	Industrial Controls
Interfaces	System engineer	Verification procedure	Industrial Controls
List of stakeholders	System engineer	Controls User Manual	Industrial Controls

- Presented to PIP-II project management on behalf of the Industrial Controls group
 - Full credit: At the request of the project managers!
- Sets expectation for what information my team needs before proceeding with system design.
 - Working with half-baked information makes it likely we will be redesigning in the future.
- Standard templates for all documents listed here.
 - Mostly. Work in progress.

A grayscale photograph of the interior of a particle accelerator tunnel, showing the complex machinery and the perspective of the tunnel's length.

Thank you.

Questions or suggestions?