AUTHENTISE

Weaving the Digital Thread

Eli Ribble

Background - Eli Ribble

MSc from University of Utah

Built simulations platform at L3 (MPRI)

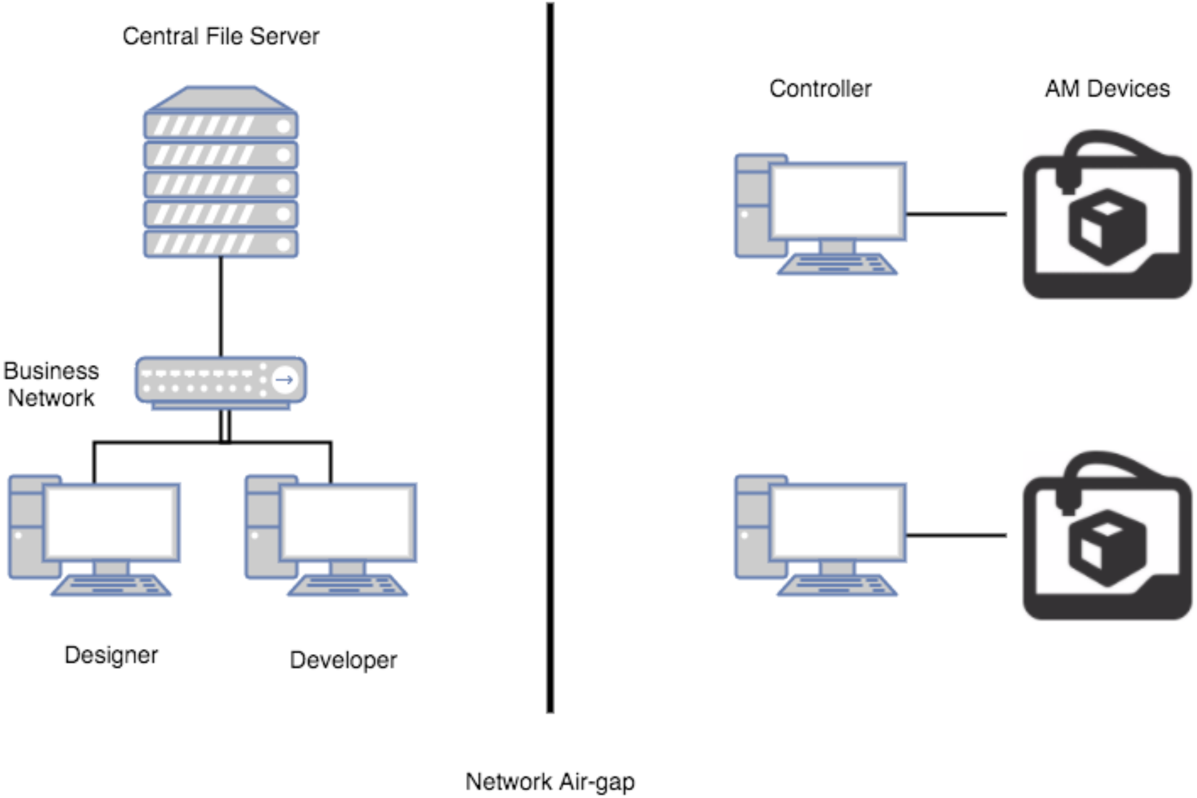
Built digital assessment platform at HireVue

CTO at Authentise

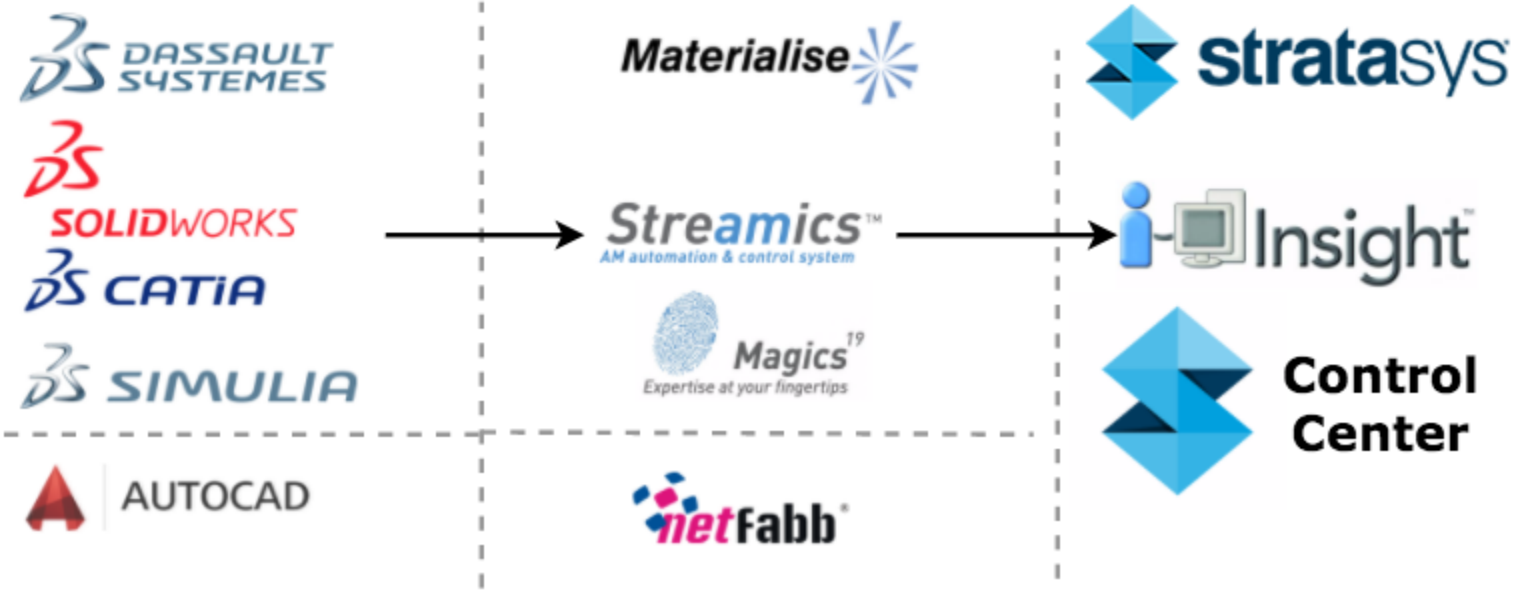
Background - Authentise

- Started in secure digital streaming and DRM
    - Worked with 67 partners around the world - Lowes, Stratasys, HP
- Services division to tailor solutions for major customers
    - Partnered with WiPro
- From there built a platform on discrete services for Digital Manufacturing
    - 30 different modules - nesting, rendering, toolpath generation, in-process monitoring
    - Modules are separable, composable and integrate with 3rd parties

Hardware Layout



Software Layout

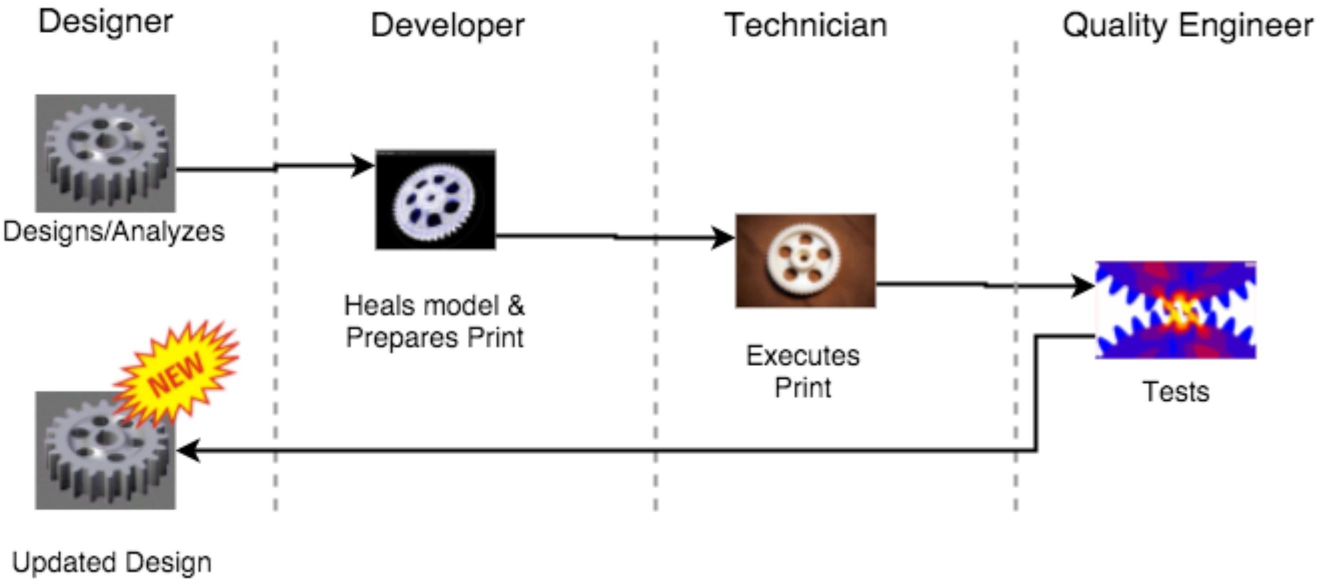


Design

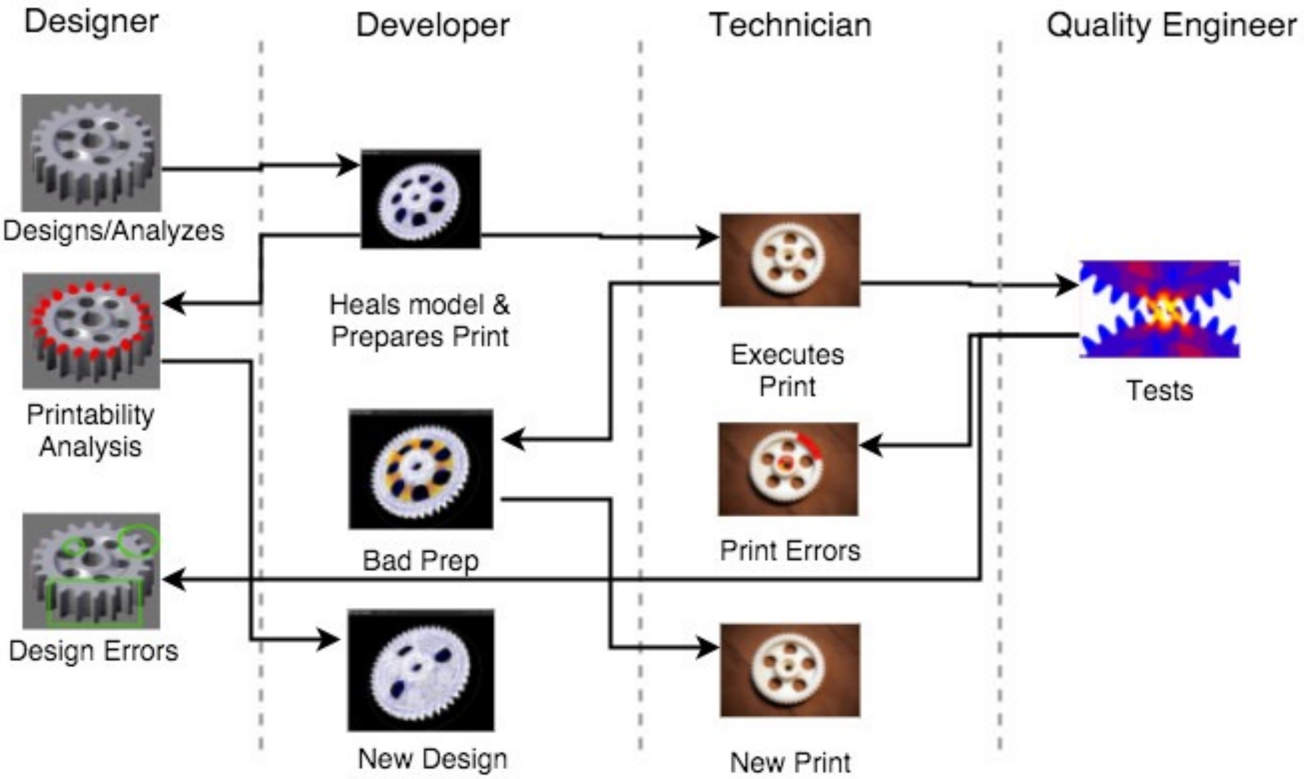
Preparation

Implementation

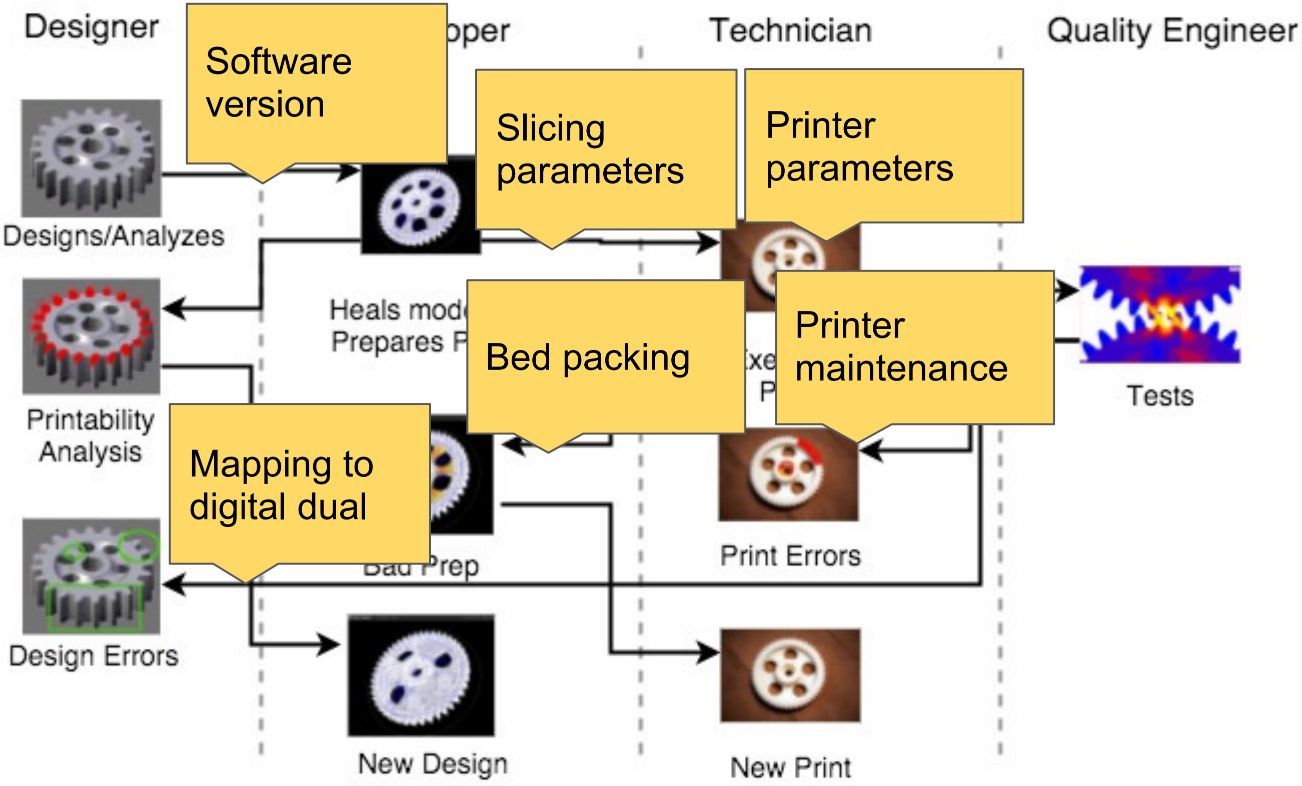
Ideal Time Series



Actual Time Series



Issues Through Time



Software version

Slicing parameters

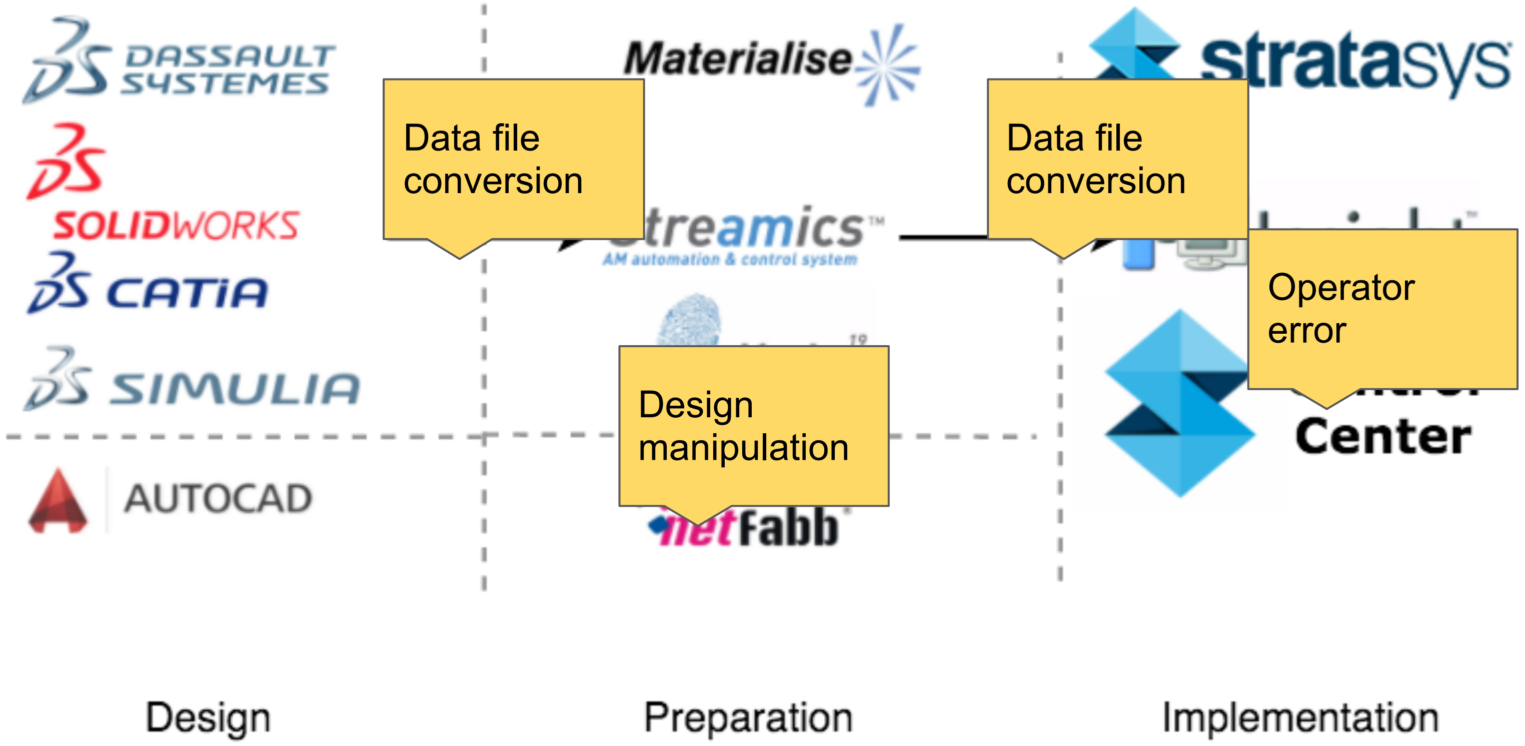
Printer parameters

Bed packing

Printer maintenance

Mapping to digital dual

Issues Through Software



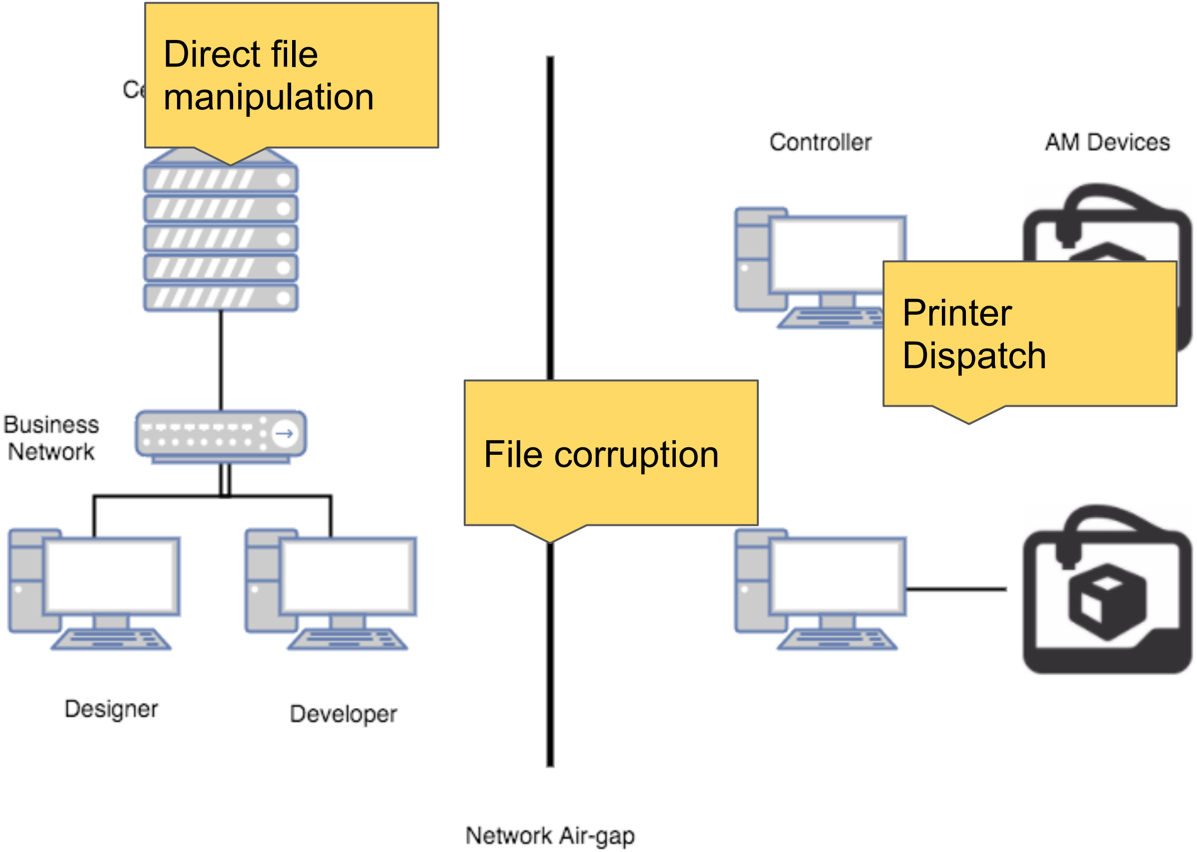
Data file conversion

Data file conversion

Operator error

Design manipulation

Issues Through Hardware



Direct file manipulation

File corruption

Printer Dispatch

Major Issues

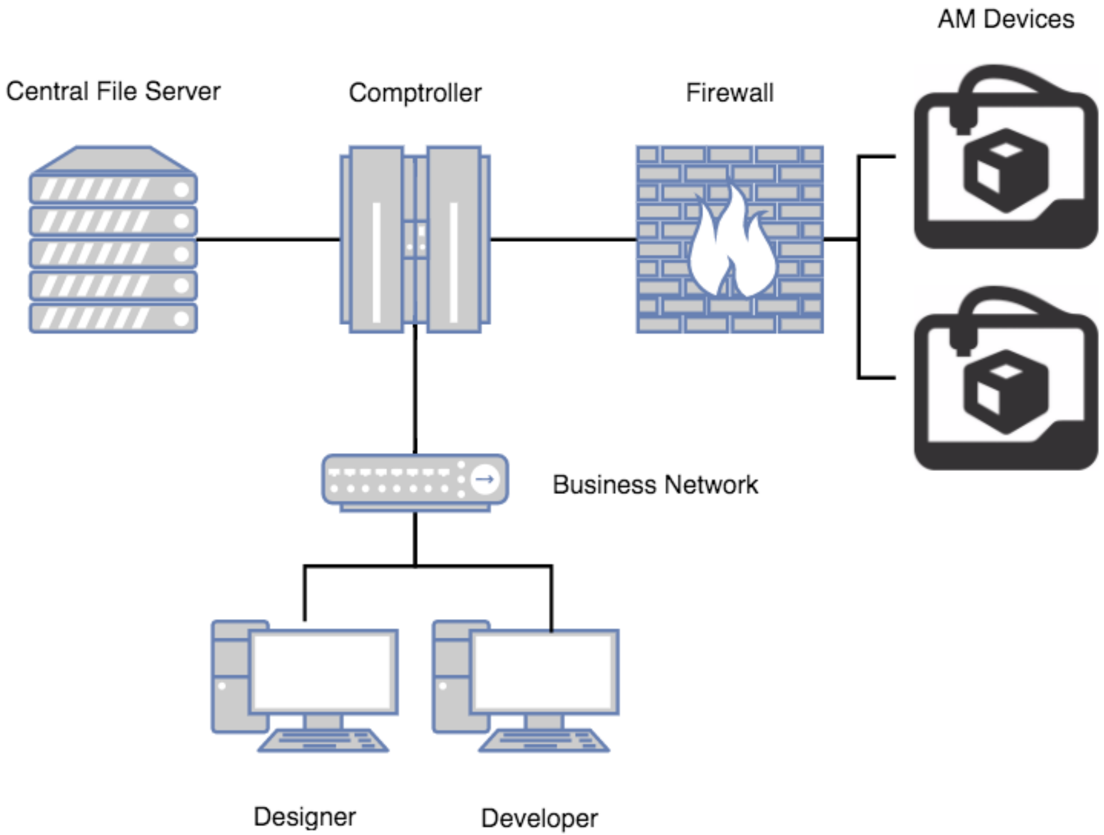
- Traceability - Who did what to the design when based on what feedback?
  - Extending the control loop
- Fidelity - Is the product produced representative of the design?
  - Regulatory compliance
- Security - Was the initiator of change properly permitted to do so?
  - Role-based computing
  - IP Protection

Rebuilding from the ground up

- Air-gapping decreases security
  - Two networks with separate policies
  - Duplicate monitoring resources
  - Extremely hard to track legitimate actions cross-gap
- Common filesystems are too flexible
  - Coordinating revisions requires coordinating people and practices
  - Un-intelligent auditing
  - Policy is the only thing keeping related assets together
- AM device state is a black box
  - Only a few trained technicians know about or deal with AM devices
  - Those who interact with AM devices are layers removed from those who design its output

Updated Hardware Layout

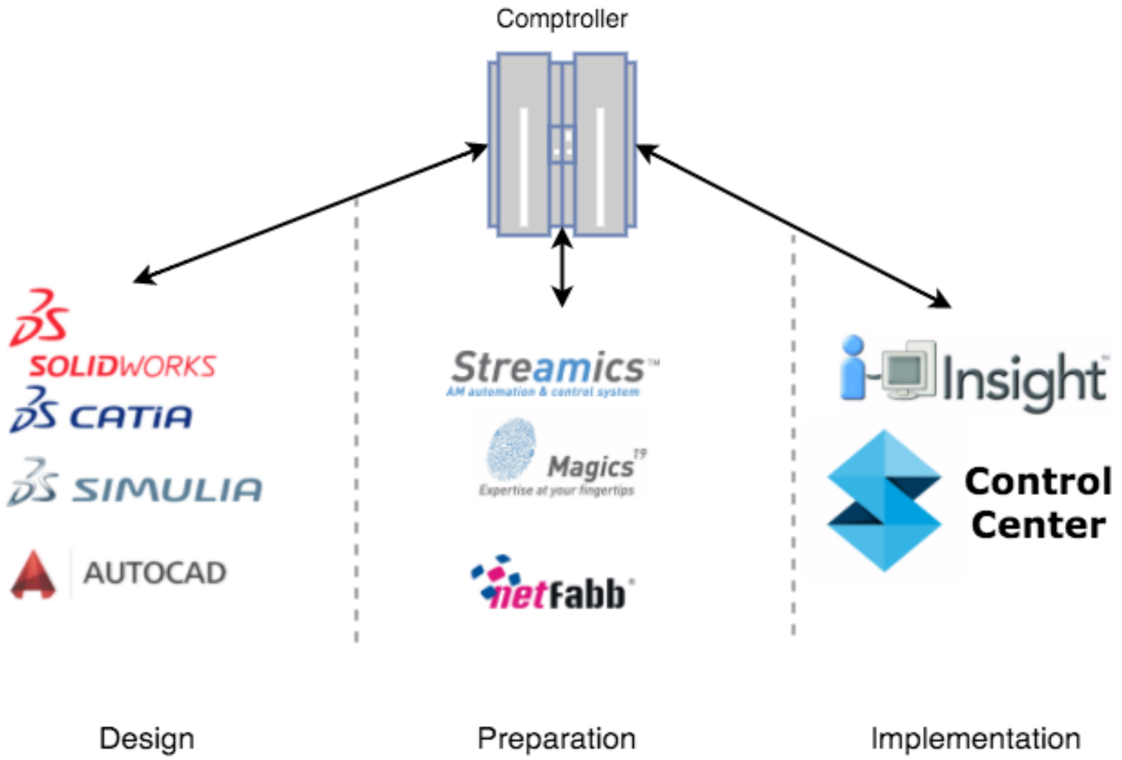
- Central CAM File Server is only accessible to the Comptroller
- All CAM data access goes through the Comptroller
- No air-gap. Printers are networked, but properly firewalled
- All AM Device access goes through the comptroller and the device firewall



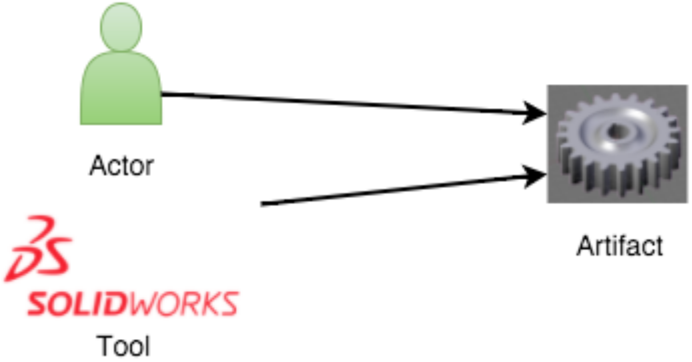
AUTHENTISE

Updated Software Layout

- All CAM data access goes through the Comptroller
- Workflow tools must send output to the Comptroller
- Instructions to printer must go through the Comptroller

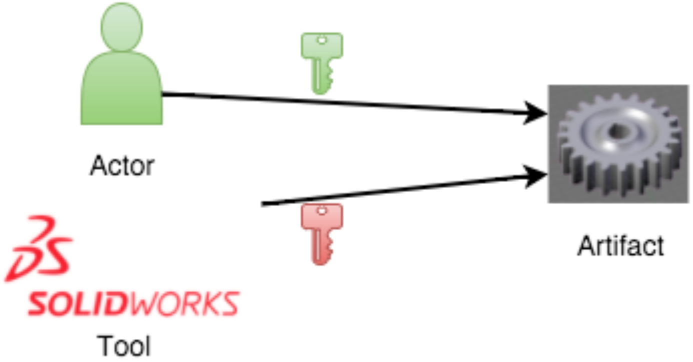


Asset Creation 1



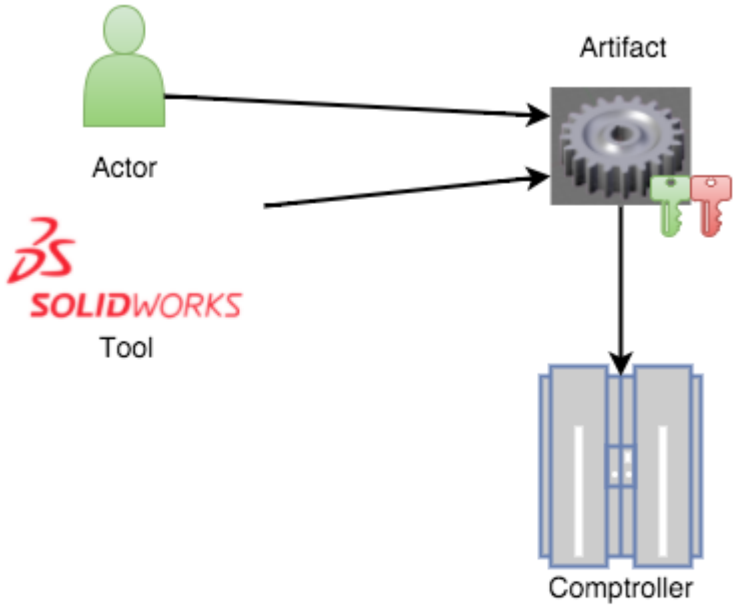
And Actor uses a Tool, such as SolidWorks, to produce an artifact. This artifact is entirely new and therefore has no history

Asset Creation 2



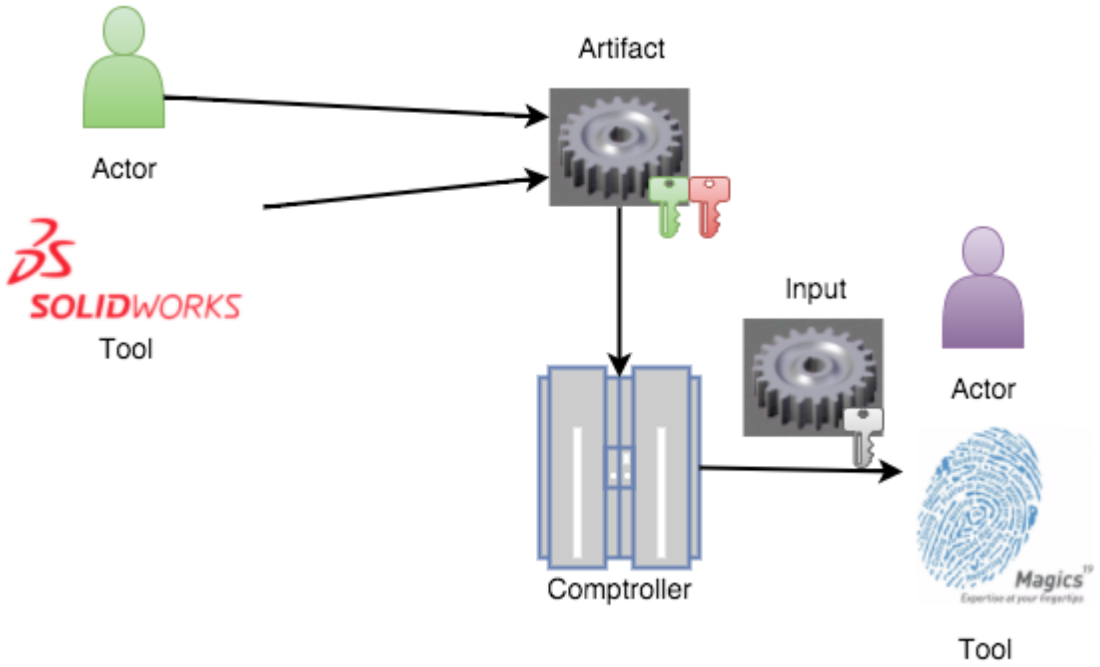
The Actor cryptographically signs the artifact with a personal key
The Tool cryptographically signs the artifact with a version-specific key
This cryptographically guarantees the ‘who’ and the ‘how’

Asset Creation 3



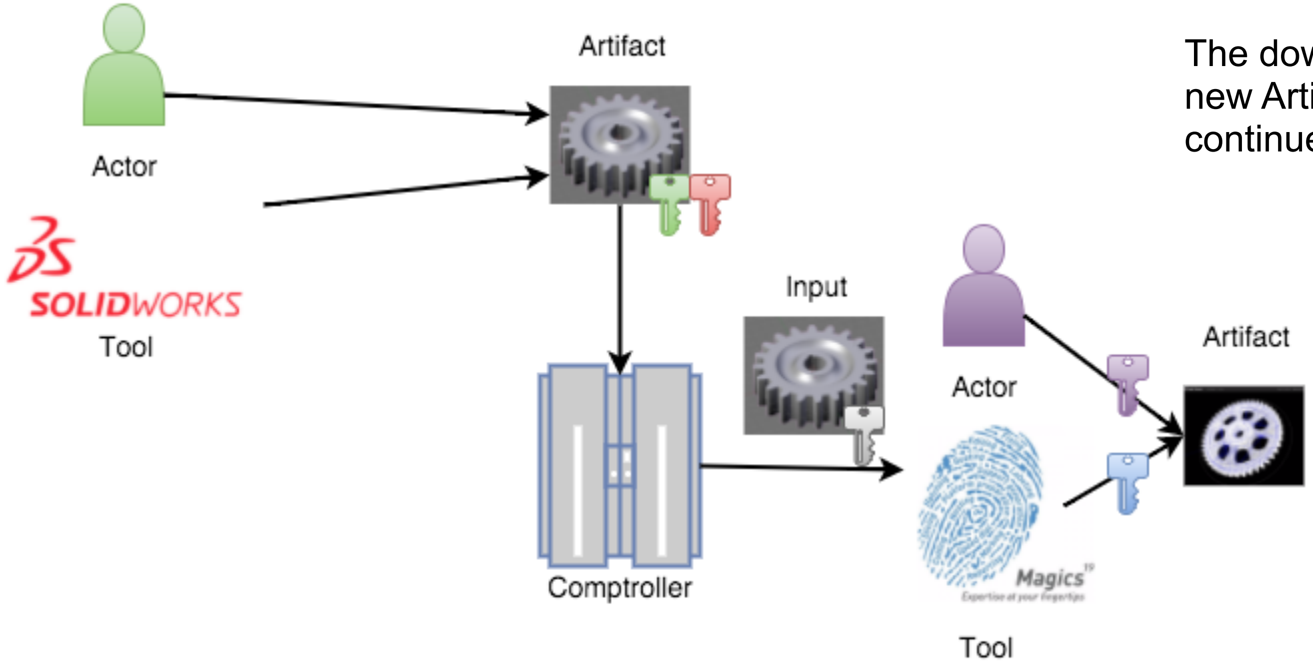
Together these keys and the artifact certify to the Comptroller the origin of a new asset

Asset Creation 4



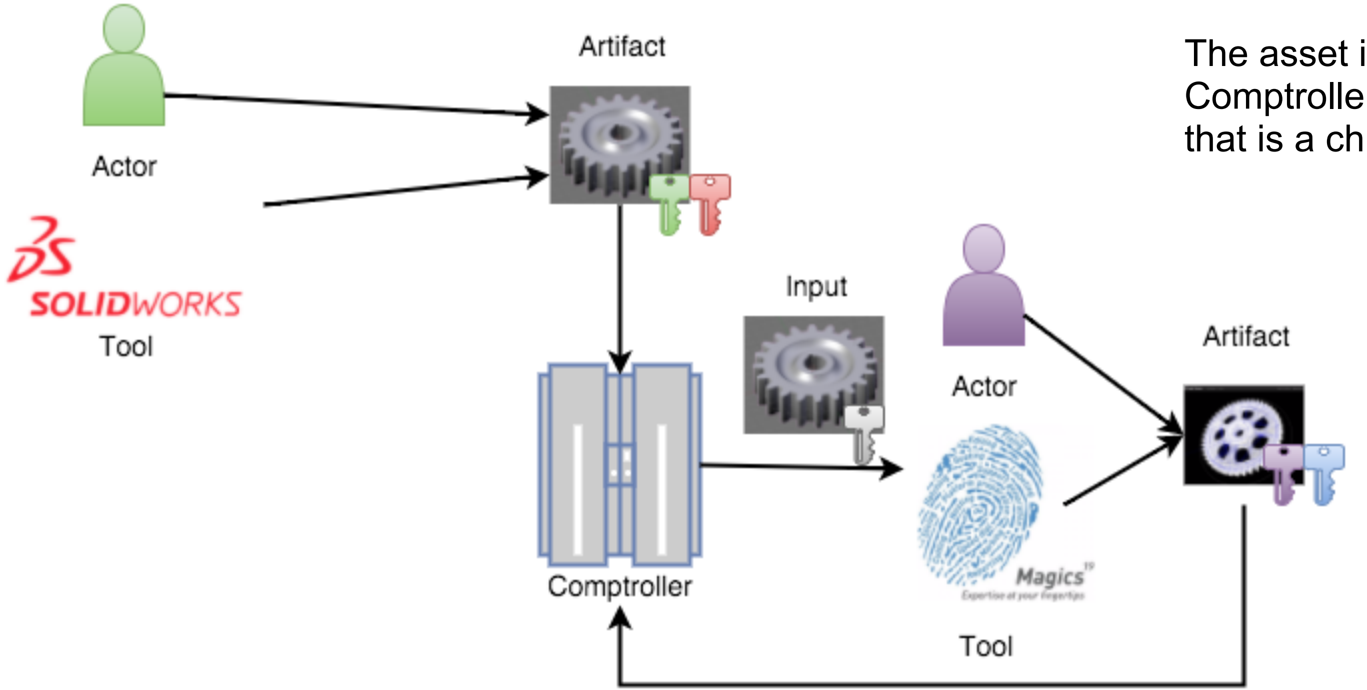
The Comptroller signs the asset and makes it available to a new Actor through a secure channel working on a new tool in a downstream process.

Asset Creation 5



The downstream Actor and Tool sign new Artifacts that are produced to continue the chain of provenance

Asset Creation 6



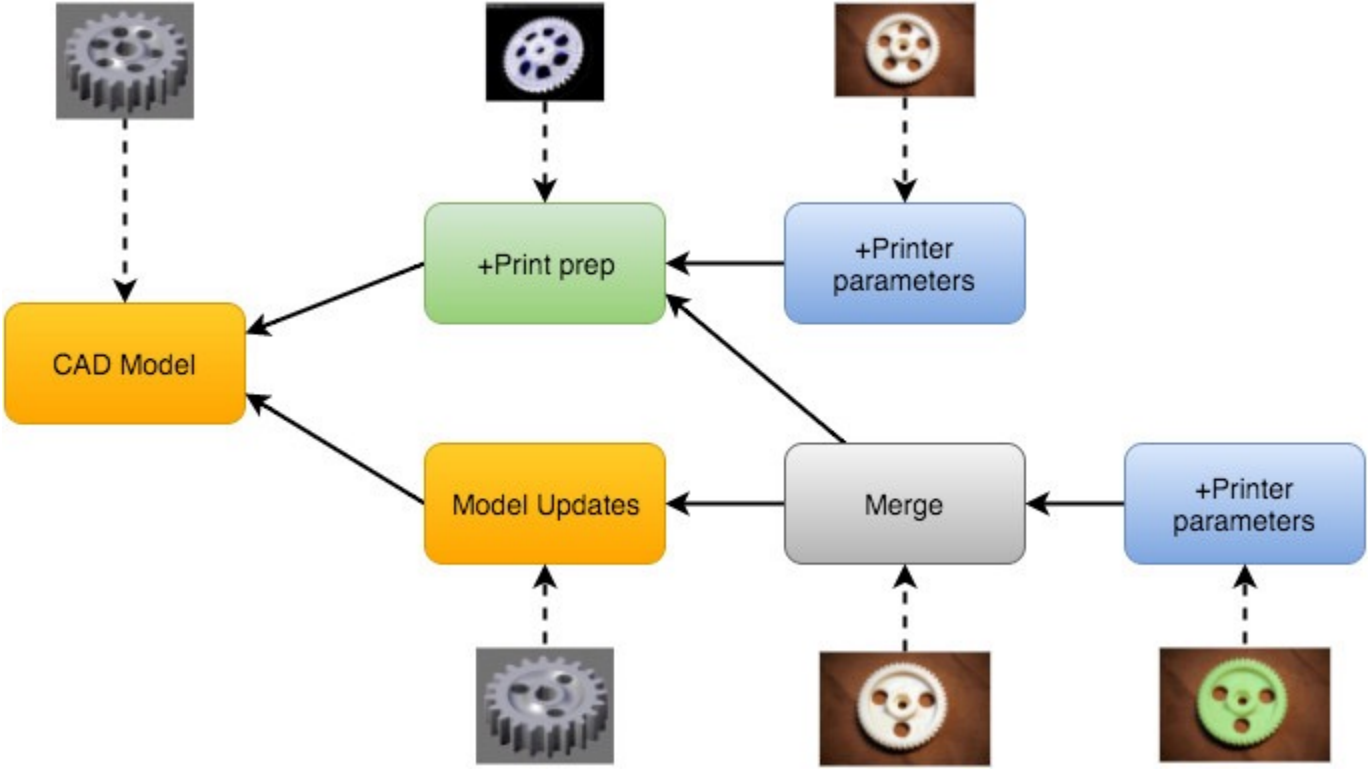
The asset is updated by notifying the Comptroller of a newly signed artifact that is a child of the original asset

Signed Part History

Every change or usage of an asset becomes part of network of changes showing precise history

Cryptographic signatures guarantee integrity of provenance data

This includes signatures from AM Devices that manufacture parts

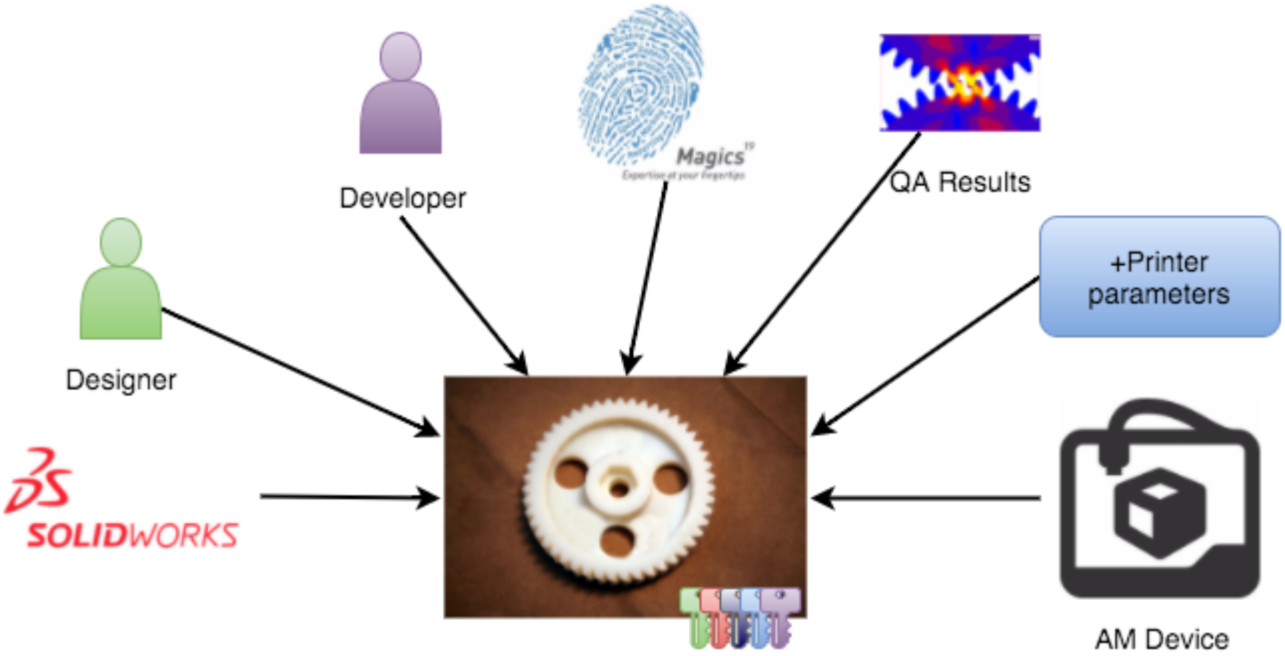


Provenance

Every part maintains a cryptographically secure provenance document

Includes AM Device signature and parameters at moment of creation

Provenance can be augmented post-production with QA analysis



Security Considerations

Each tool in the chain receives instructions from a user, a user’s key and data inputs from the Comptroller

The Comptroller can deny actions

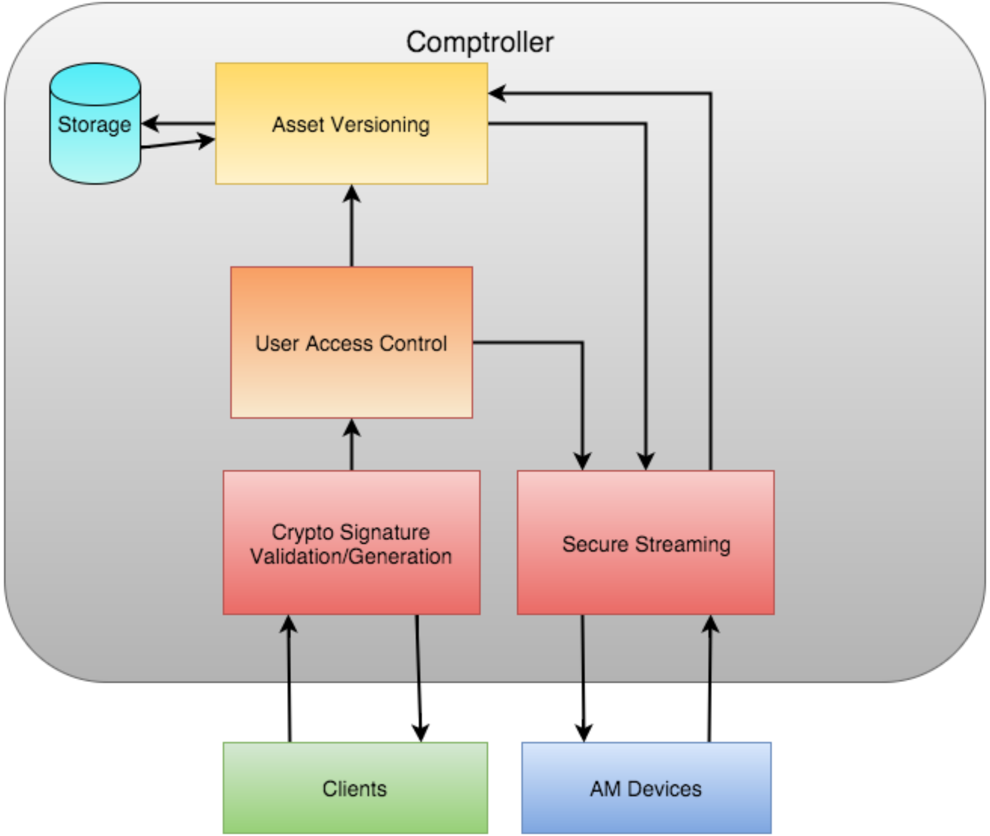
- User’s roles
- Organization policies
- Failed intrusion detection checks
- Content-creator imposed constraints (DRM)

The Comptroller validates new artifact signatures to identify tool tampering

Comptroller Internals

Comptroller is conceptually, not architecturally monolithic

High availability and scalability can be applied to each component separately



Comptroller in the large

Systems can be created between organizations by allowing Comptrollers to communicate

Requests for data and updates are handled cross-organization via the same key/signature mechanisms

IP protection is handled by controlling data access and artifact creation

Requests for changes in ownership become part of the provenance chain

Required Components

Cooperation from AM Device OEMs for parameter capture & control, secure streaming

Standards agreement between software providers on crypto signature

Plugins for data file transport to/from Comptroller

Drawbacks

Single point of failure: Comptroller

- Mitigation: separate components, scale independently

Intrusion detection is harder than air gapping

- Mitigation: Standardization of approaches means you don't, and shouldn't, do it alone

Crypto means more steps in an already long process

- Mitigation: Automation and good tool support makes this invisible. How hard is SSL?

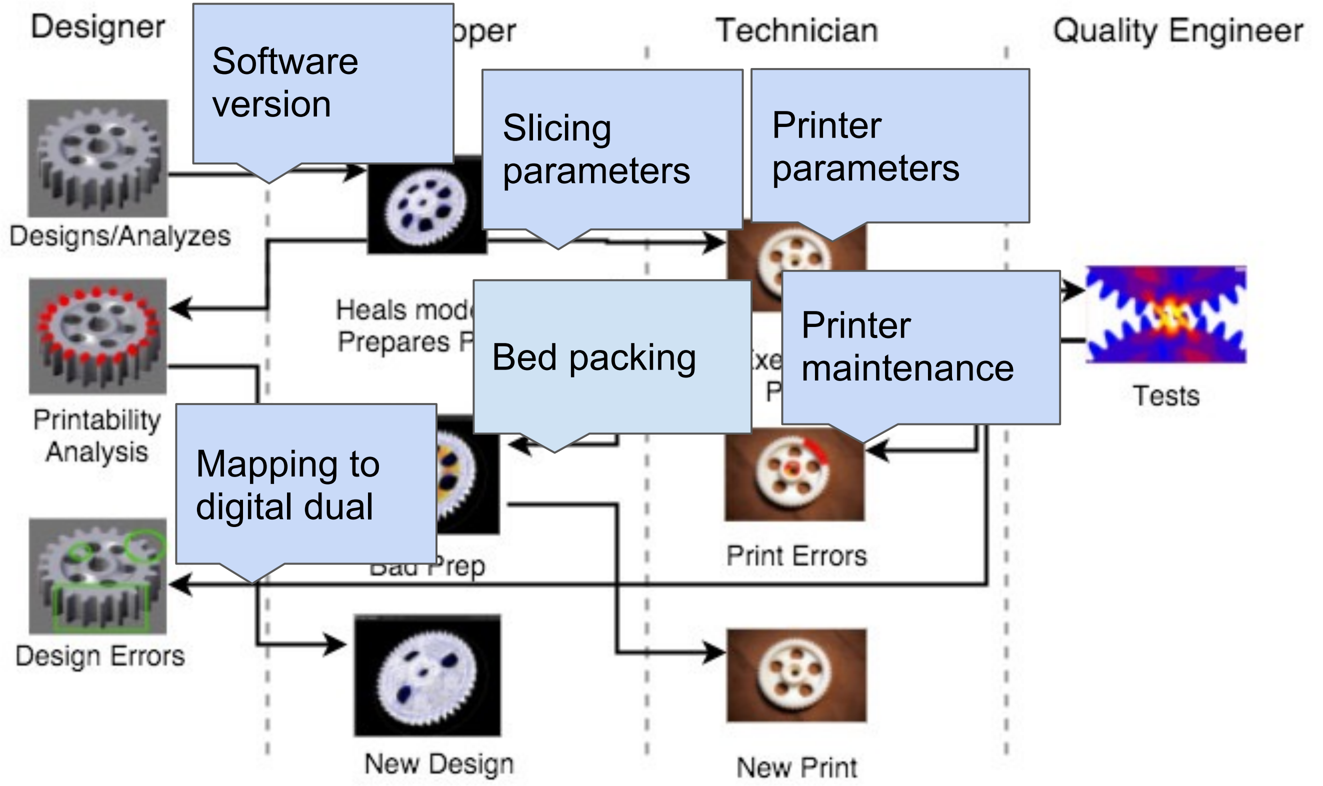
No offline mode

- Mitigation: Signatures can be baked into open file formats, public keys can be locally cached and validated, actions for Comptroller can be queued

Does not address physical security

- True, but it is better at detecting breach, nefarious modification and sabotage

Issues through Time - Revisited



Software version

Slicing parameters

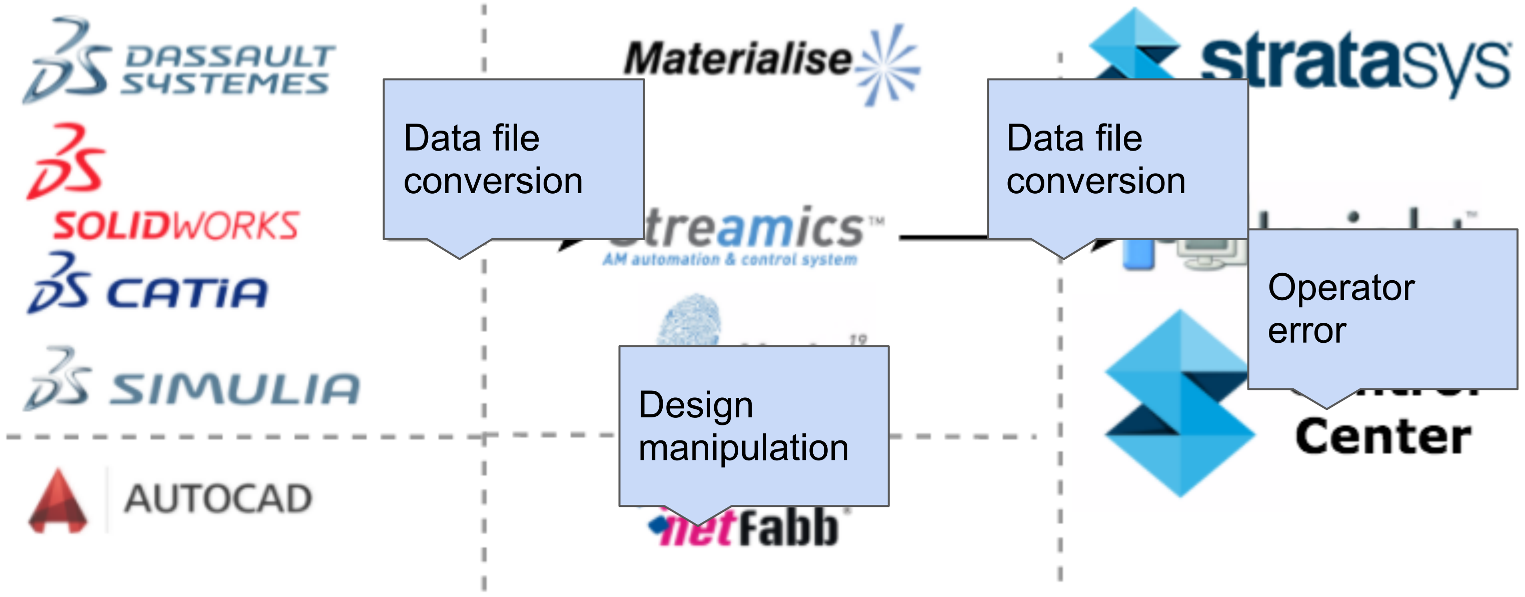
Printer parameters

Bed packing

Printer maintenance

Mapping to digital dual

Issues through Software - Revisited



Data file conversion

Data file conversion

Operator error

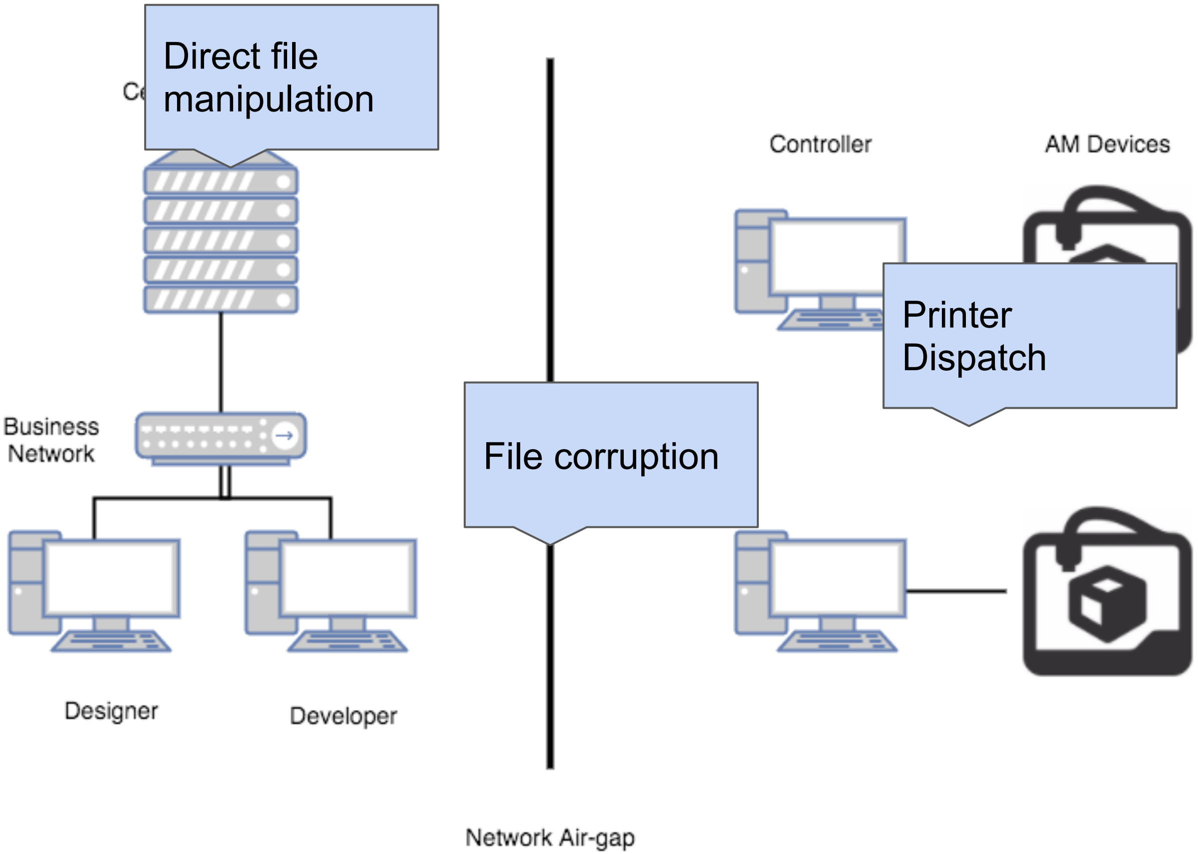
Design manipulation

Design

Preparation

Implementation

Issues Through Hardware



Direct file manipulation

Printer Dispatch

File corruption

Major Issues Revisited

- Traceability - Who did what to the design when based on what feedback?
  - Cryptographic signatures ensure who and the what and the when
  - Automatic history indicates feedback used at each step - QA, device parameters, etc
- Fidelity - Is the product produced representative of the design?
  - New design versions pushed down to devices
  - Device feedback pushed up to designers
- Security - Was the initiator of change properly permitted to do so?
  - Crypto keys authenticate user and tool
  - Authorization at each asset change
  - Direct control of AM Device detects and prevents hardware exploits

Conclusions

A unidirectional data flow between vendor silos cannot scale

Embracing interconnected tools enhances security, fidelity and traceability

Cryptographic keys leave processes flexible while maximizing centralized control and asset management.

Security-in-depth vs perimeter security

Feedback data should be automatically matched to asset versions