STPA For Additive Manufacturing Software

STAMP Workshop, MIT, March 22, 2016

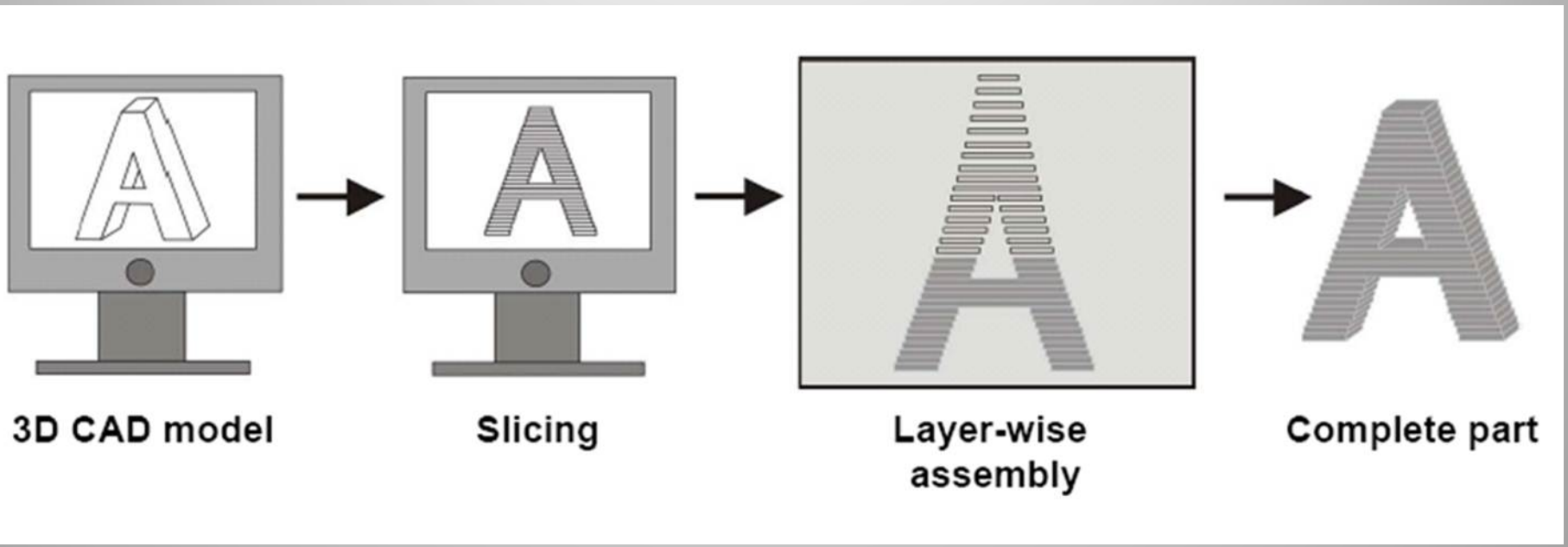
Gregory Pope

Lawrence Livermore National Laboratory

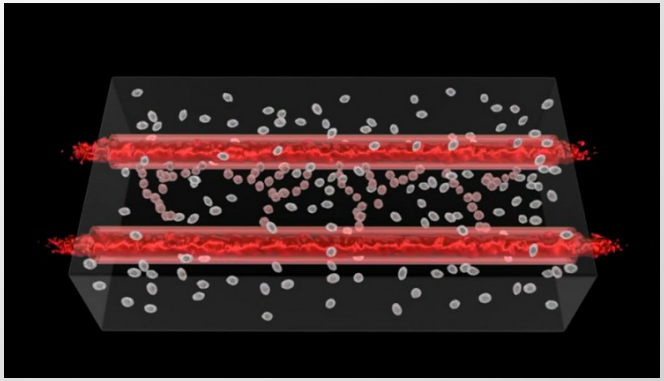
LLNL-PRES-685389

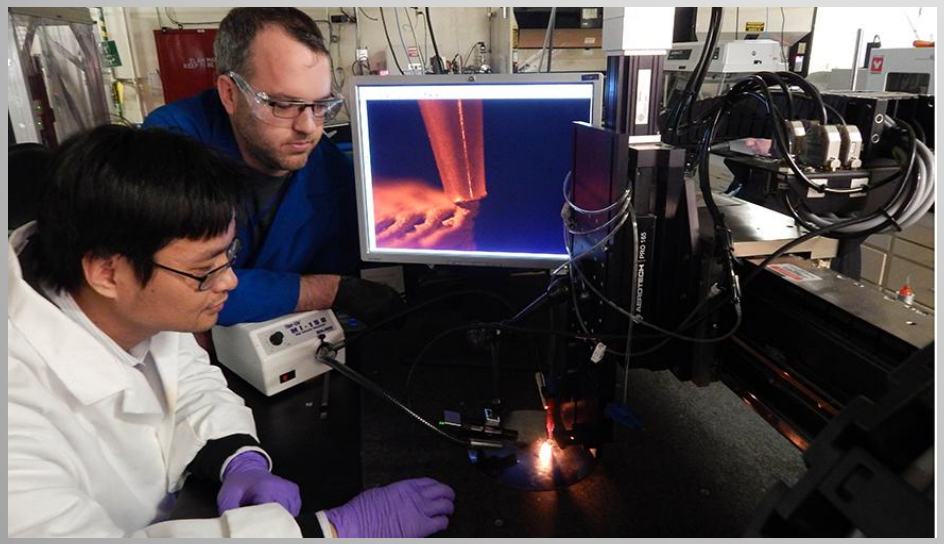
This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

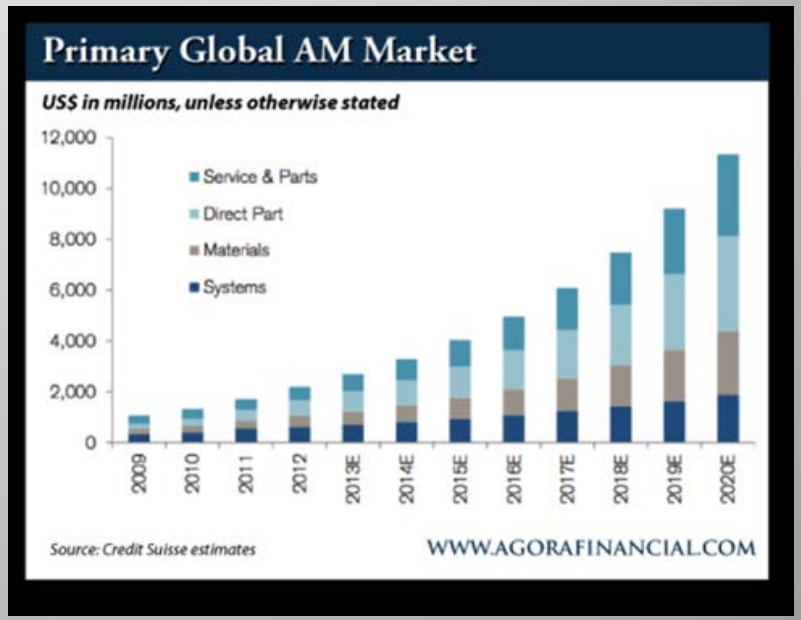
AM Has Four Basic Steps



AM Applications Doubling by 2020

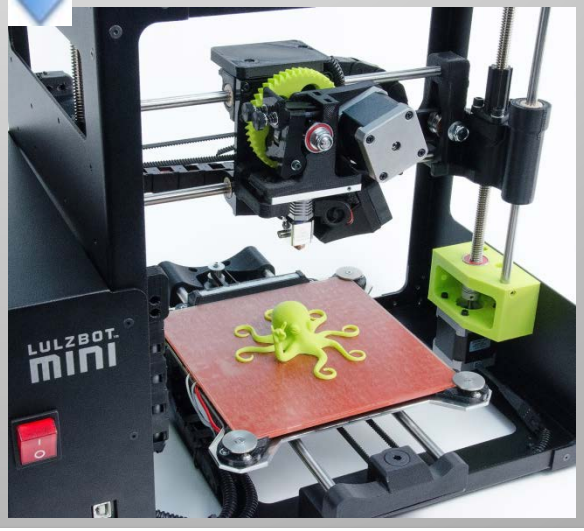






Currently Hobby Level 3D Printer Hardware and Software

Printer Software



And Industrial Strength 3D Printing Hardware and Software

Future Pilot Announcement: Ladies and Gentlemen our flight has been delayed waiting for the remainder of our right engine's parts to be printed and installed.

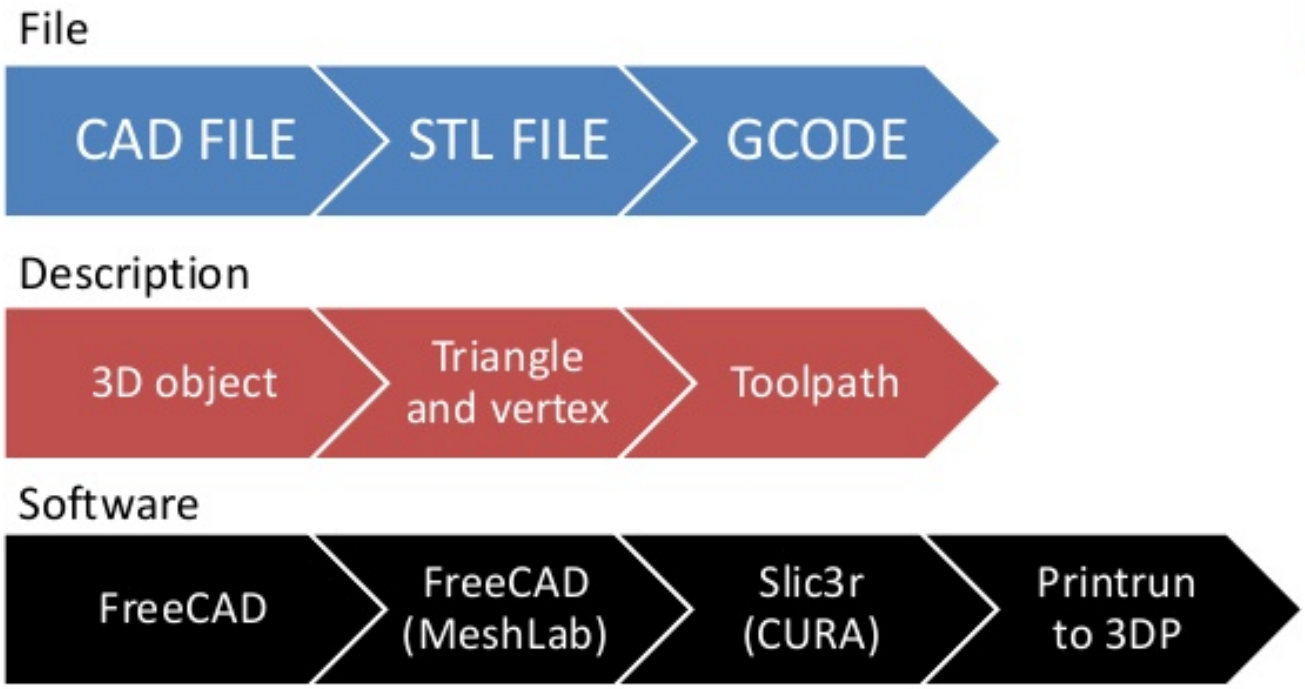
MONASH University

There are Multiple 3D Printer Technologies

Printing Technique	Hazardous Materials Used
Stereo Lithography(SLA)	Molten Plastic
Digital Light Processing(DLP)	Heat, Inert Gas
Fused Deposition Modeling (FDM)	Heat
Selective Laser Sintering (SLS)	Laser, Powders
Selective Laser Melting (SLM)	Laser, Metallic Powders, Gases
Electronic Beam Melting (EBM)	Electron Beam, High Voltage
Laminated Object Manufacturing (LOM)	Laser, Sound

Software and Data Heavily Used

Additive manufacturing Process Flow



Numerous 3D Printer Software Makers


AUTODESK 123D


SketchUp

Beginner → Advanced


FreeCAD


SCULPTRIS


3DTin


OpenSCAD


3DS MAX


AUTOCAD


CINEMA 4D

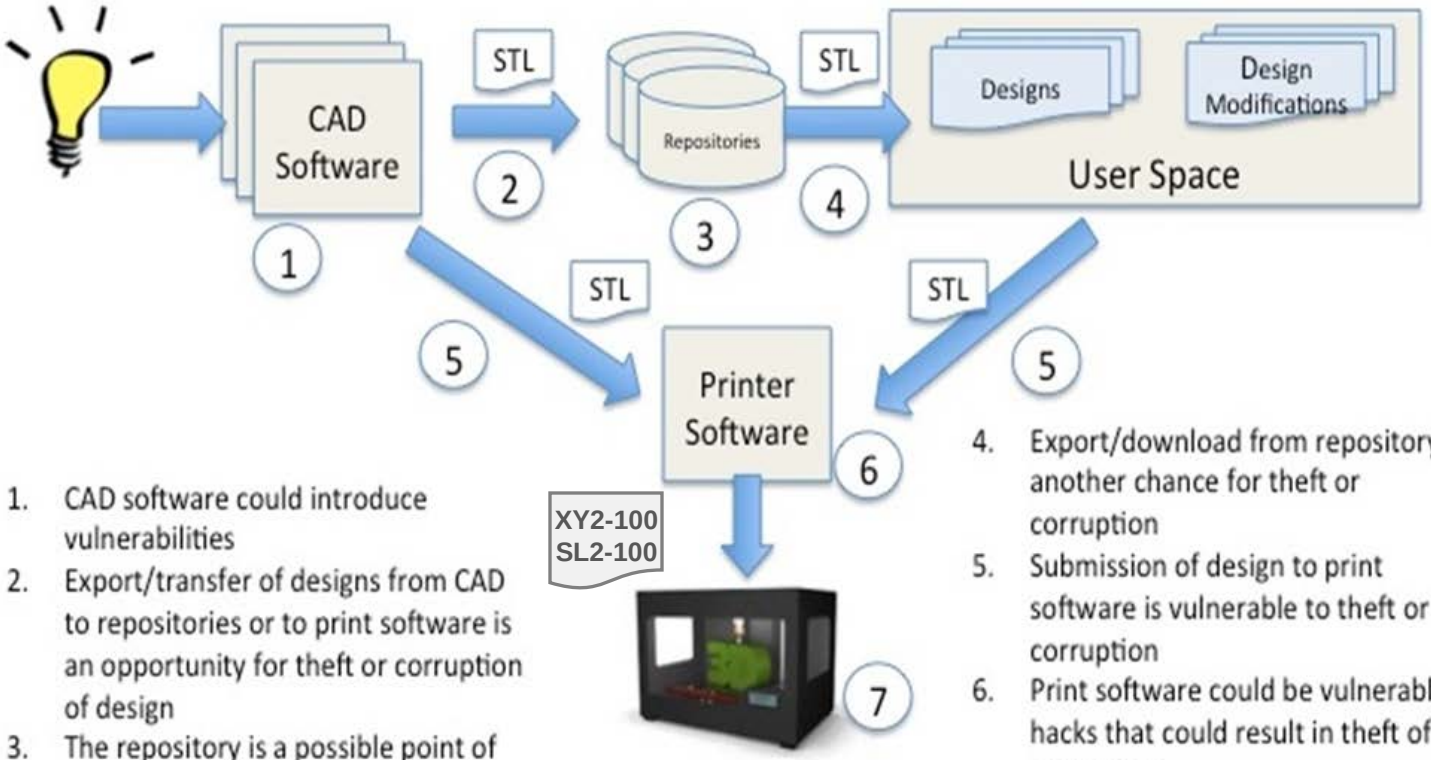

LightWave


blender

Expert Analysis from Literature

- "Additive Manufacturing Security", University of Alabama Huntsville
- "Security Challenges with Additive Manufacturing with Metals and Alloys" Yampolskiy, Schutzle, Vaidya and Yasinsac

Additive Manufacturing Security



1. CAD software could introduce vulnerabilities
2. Export/transfer of designs from CAD to repositories or to print software is an opportunity for theft or corruption of design
3. The repository is a possible point of theft or corruption of design
4. Export/download from repository is another chance for theft or corruption
5. Submission of design to print software is vulnerable to theft or corruption
6. Print software could be vulnerable to hacks that could result in theft of corruption
7. Printer system software and the transfer to it, are potential points of theft or corruption

Susan M. Bridges
University of Alabama in Huntsville
S347 Technology Hall
Huntsville, AL 35899
256-824-5143
sbridges@itsc.uah.edu

Sara J. Graves
University of Alabama in Huntsville
S339A Technology Hall
Huntsville, AL 35899
256-824-6064
sgraves@itsc.uah.edu

Ken Keiser
University of Alabama in Huntsville
S343 Technology Hall
Huntsville, AL 35899
256-824-6825
keiserk@itsc.uah.edu

Nathan Sissom
University of Alabama in Huntsville
S347 Technology Hall
Huntsville, AL 35899
256-479-8488
nsissom@itsc.uah.edu

Cyber Attack Vectors

- Supply Chain Attacks
- Software and Firmware Updates
- Code Injection
- Modification of 3D Models
- Manufacturing Process Specification

SECURITY CHALLENGES OF ADDITIVE MANUFACTURING WITH METALS AND ALLOYS
Mark Yampolskiy, Lena Schutzle, Uday Vaidya and Alec Yasinsac

Impact on Manufacturing Parameters

- 3D Shape
- Manufacturing Orientation
- Powder Deposition
- Wire Feed Speed
- Targeting and Positioning System
- Fusing Material Patterns
- Timing
- Support Material
- Source Material
- Powder Recycling
- Temperature Control
- Heat Sources
- Chamber Atmosphere
- Post-Processing

SECURITY CHALLENGES OF ADDITIVE MANUFACTURING WITH METALS AND ALLOYS
Mark Yampolskiy, Lena Schutzle, Uday Vaidya and Alec Yasinsac

Cyber Security Conclusions

- Keep AM air gapped to Internet
  - Avoids cyber attacks
  - Avoids cyber theft

- Can STPA tell us anything else we should be aware of?
  - Risks for printed parts
  - Hazards for printed mission critical parts
  - Hazards for printing process
  - Additional security vulnerabilities

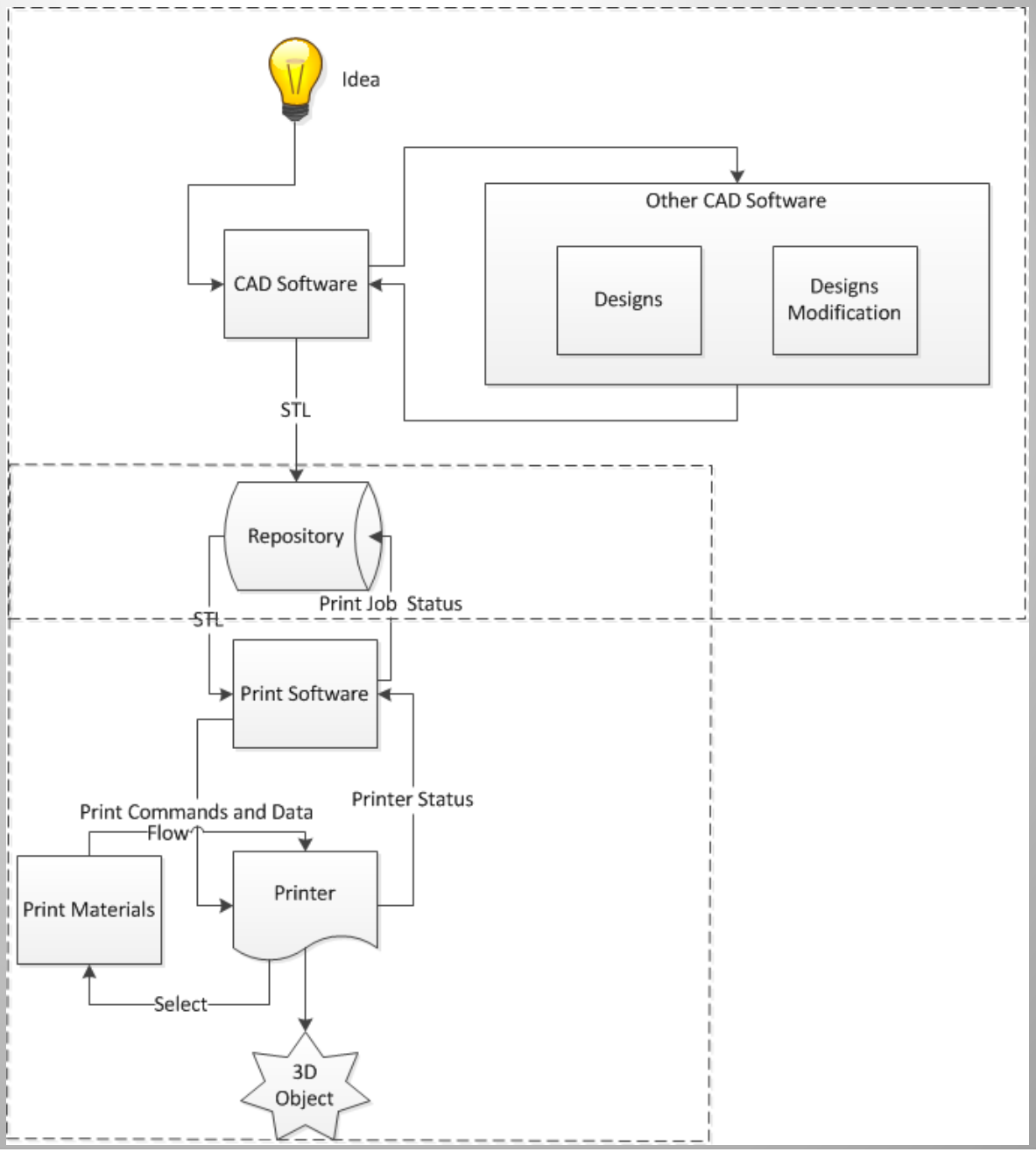
Is STPA Useful in Additive Manufacturing Analysis?

- For Identifying:
  1. Software System Risks
  2. Software System Hazards
  3. Cyber Security Vulnerabilities

- Approach:

  Compare STPA analysis results done by AM novice to published works of AM experts.

STPA System Model



CAD Subsystem

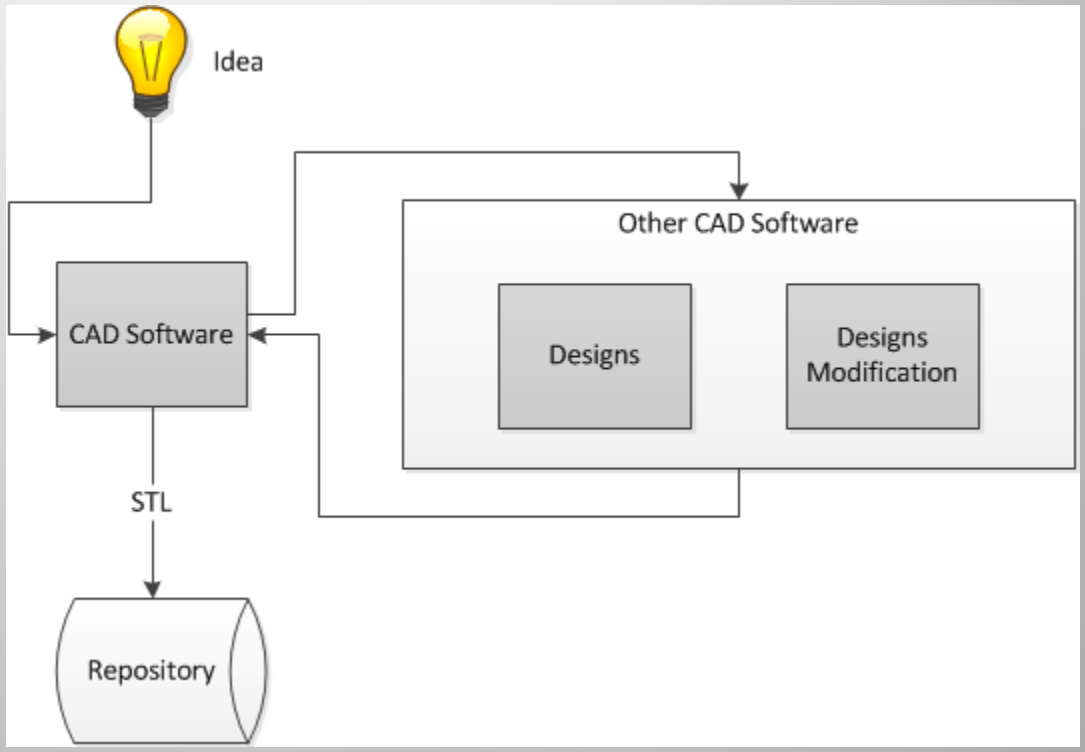
STPA Guide Phrases

A resource or action required for correct operation is not provided or is not followed.

An incorrect resource or action is provided that leads to a hazard/risk.

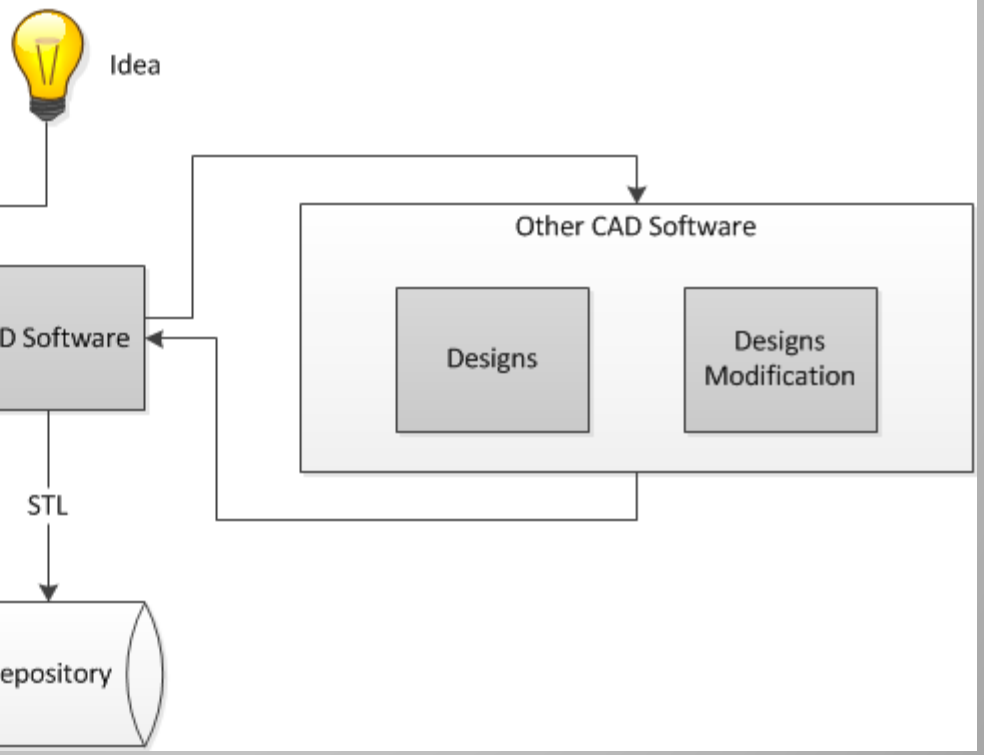
A potentially correct resource or action is provided too late, or out of sequence.

A correct resource or control action is stopped too soon or applied too long.



CAD Subsystem Hazards/Risks (16)

Software has bug
Software update has bug
Support software has bug
Software has exploitable vulnerability
Support software has exploitable vulnerability
Version incompatibility
Resolution or precision incompatible with manufacturing tolerances
Design contains errors not caught
User misunderstands feature behavior
Representation does not mimic materials
Design not peer reviewed
Software unable to describe design intent
Error message misunderstood by user
Error message overlooked by user
Error correction not saved
Wrong design or version sent to repository



Repo Subsystem

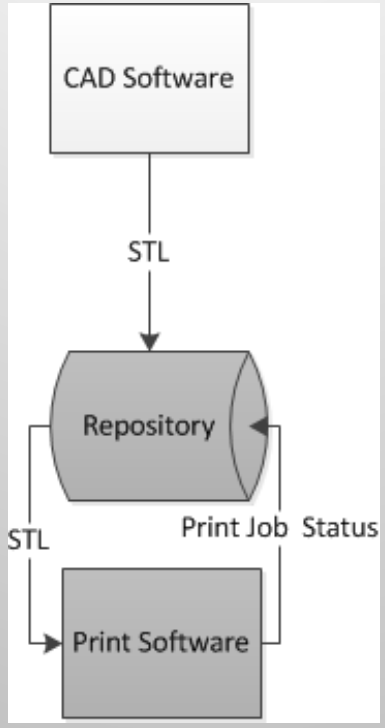
STPA Guide Phrases

A resource or action required for correct operation is not provided or is not followed.

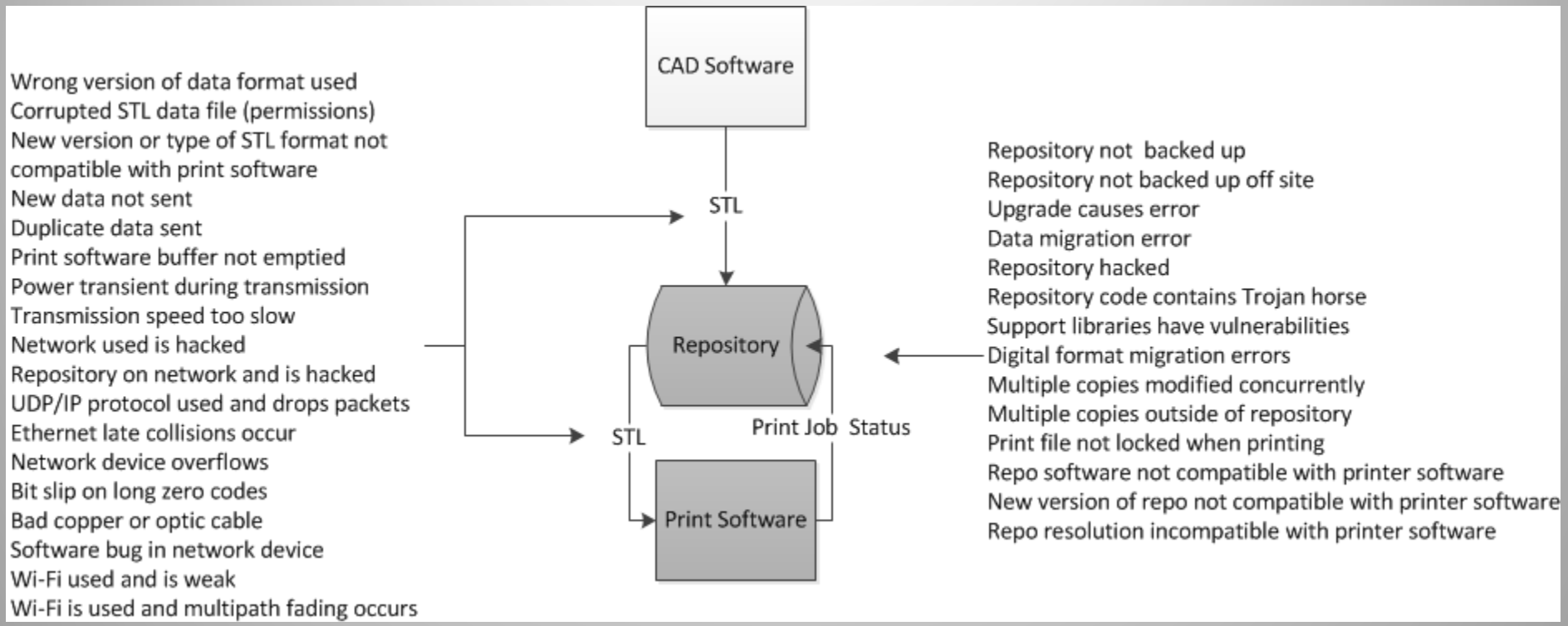
An incorrect resource or action is provided that leads to a hazard/risk.

A potentially correct resource or action is provided too late, or out of sequence.

A correct resource or control action is stopped too soon or applied too long.



Repo Subsystem Hazards/Risks (32)



STL (Standard Tessellation Language) ASCII Format

An ASCII STL file begins with the line

solid name
where name is an optional string (though if name is omitted there must still be a space after solid). The file continues with any number of triangles, each rep[illegible]ws:

Numbers can not be negative

facet normal ni [illegible]
  outer loop
    vertex v1x v1y v1z
    vertex v2x v2y v2z
    vertex v3x v3y v3z
  endloop
endfacet

Numbers in 2.6480000e-002 format

where each n or v is a floating-point number in sign-mantissa-"e"-sign-exponent format, e.g., "2.648000e-002" (noting that each v must be non-negative). The file concludes with endsolid name

STL BINARY Format

Should not begin with SOLID

Unsigned 4 byte integer max = 4,294,967,295

32 Bit Floating Point Numbers max = 2,147,183,647

UINT8[80] – Header
UINT32 – Number of triangles

foreach triangle
REAL32[3] – Normal vector
REAL32[3] – Vertex 1
REAL32[3] – Vertex 2
REAL32[3] – Vertex 3
UNIT16 – Attribute byte count
end

Unsigned 2 byte integer max = 65, 535 but should be zero in standard format

3D Printing Subsystem

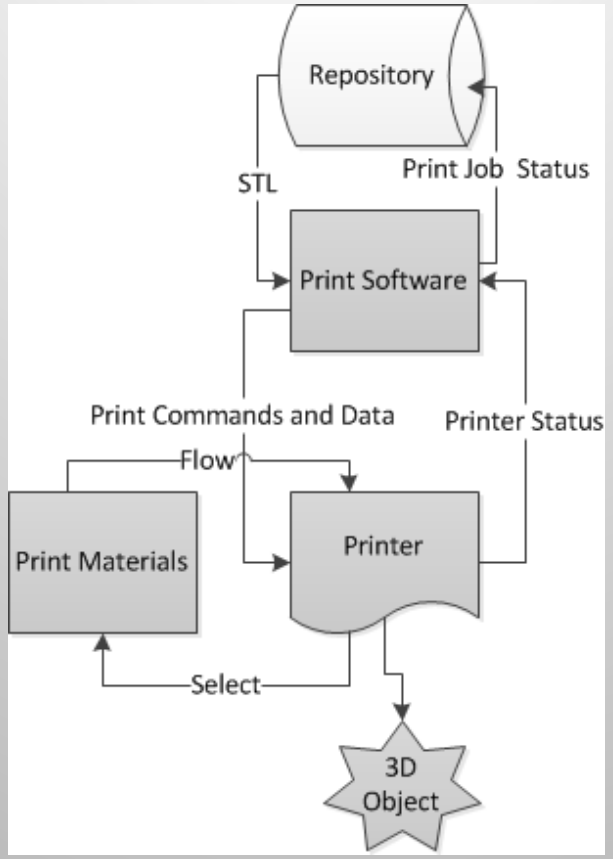
STPA Guide Phrases

A resource or action required for correct operation is not provided or is not followed.

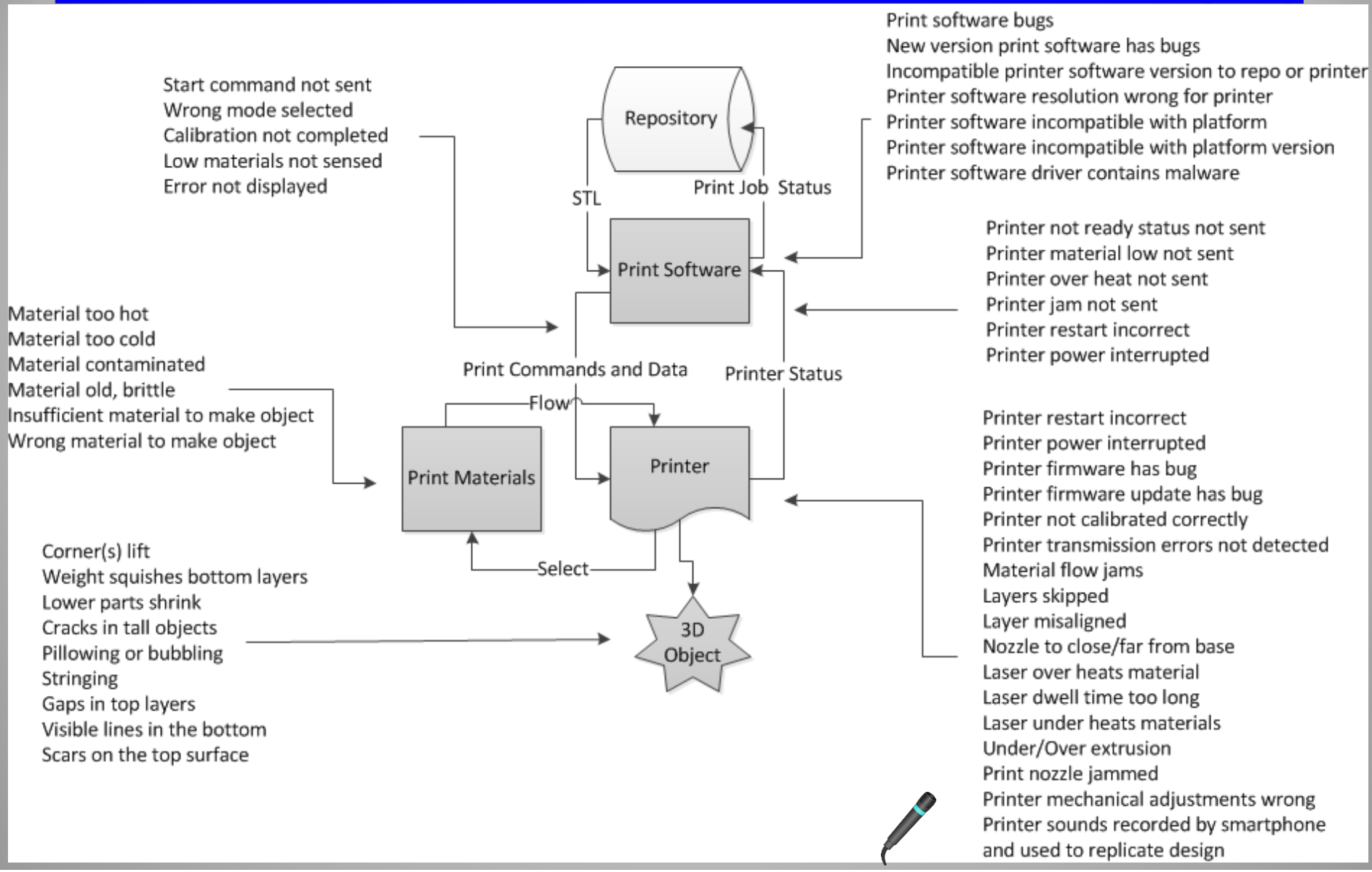
An incorrect resource or action is provided that leads to a hazard/risk.

A potentially correct resource or action is provided too late, or out of sequence.

A correct resource or control action is stopped too soon or applied too long.



3D Printing Subsystem Hazards/Risks (50)



Factory Automation Software is yet to be Mission Critical Level

Application Domain	Number Projects	Error Range (Errors/KESLOC)	Normative Error Rate (Errors/KESLOC)	Notes
Automation	55	2 to 8	5	Factory automation
Banking	30	3 to 10	6	Loan processing, ATM
Command & Control	45	0.5 to 5	1	Command centers
Data Processing	35	2 to 14	8	DB-intensive systems
Environment/Tools	75	5 to 12	8	CASE, compilers, etc.
Military -All	125	0.2 to 3	< 1.0	See subcategories
▪ Airborne	40	0.2 to 1.3	0.5	Embedded sensors
▪ Ground	52	0.5 to 4	0.8	Combat center
▪ Missile	15	0.3 to 1.5	0.5	GNC system
▪ Space	18	0.2 to 0.8	0.4	Attitude control system
Scientific	35	0.9 to 5	2	Seismic processing
Telecommunications	50	3 to 12	6	Digital switches
Test	35	3 to 15	7	Test equipment, devices
Trainers/Simulations	25	2 to 11	6	Virtual reality simulator
Web Business	65	4 to 18	11	Client/server sites
Other	25	2 to 15	7	All others

Donald Reifer, "Industry Software Cost, Quality, and Productivity Benchmarks", DoD Software Tech News, July 2004

2016 Benchmark for Factory Automation Better – Donald Reifer

- Assumption is defect rate after one year, not at release as in 2004
- 2 defects per ksloc for Factory Automation codes in 2016 after one year.
- .55 defects per ksloc for Mission Critical codes
- What should defect rate be for 3D mission critical parts then?

Reifer Consultants
http://reifer.com/

STPA Lessons Learned

1. STPA facilitated me to think of hazards and risks I could not think of intuitively
2. STPA identified risks and hazards not identified in the literature search
3. STPA helped me research further important topics
4. STPA helped me ask better questions of experts

Sample of STPA Hazard Finds

1. Do not use UDP network protocol with AM (transmission not guaranteed)
2. Have printer buffers large enough to hold the entire print image (don't waste material if data error)
3. Assure the networks used have good QoS (avoid slow part data transmission due to network traffic)
4. Assure the print software can detect and then not use corrupted data
5. Offsite back up for parts data, test offsite backup
6. Air Gap AM from internet to avoid theft and malware
7. Isolate 3D printers from sound recording devices

Network Mitigations by OSI Layer for AM

Make sure application checks for errors in data integrity

Assure intellectual property protected with encryption

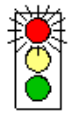
Assure 3D printer buffer large enough to hold entire image

Don't ever use UDP with AM

Use high Quality of Service network

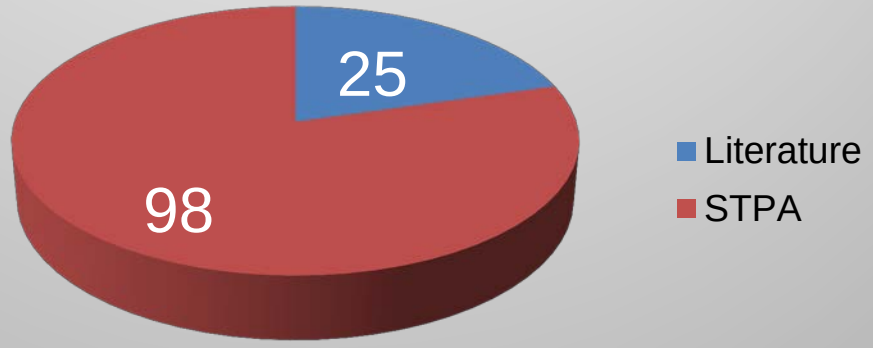
Use mature router / firewall technologies

Use fiber optic physical (emi / emc protection)

OSI MODEL			TCP / IP
7		**Application Layer** Type of communication: E-mail, file transfer, client/server.	FTP, Telnet, HTTP, SNMP, DNS, OSPF, RIP, Ping, Traceroute
6		**Presentation Layer** Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.	
5		**Session Layer** Starts, stops session. Maintains order.	
4		**Transport Layer** Ensures delivery of entire file or message.	TCP (delivery ensured) UDP (delivery NOT ensured)
3		**Network Layer** Routes data to different LANs and WANs based on network address.	IP (ICMP, IGMP, ARP, RARP)
2		**Data Link (MAC) Layer** Transmits packets from node to node based on station address.	
1		**Physical Layer** Electrical signals and cabling.	

Comparison Test

- Literature search found 25 security vulnerabilities
- STPA found 98 security vulnerabilities, hazards, and risks



Conclusion – STPA Rocks

- STPA useful addition to literature search and expert consultation for Additive Manufacturing hazard, risk, and security analysis
- STPA useful for non-real time systems analysis

Next Steps – Empirical Approach

- Mutation of 3D printer file:
  - Single bit flip
  - Word omission
  - End of transmission omission

- Assure that each seeded error is detected and data not used by 3D printer.