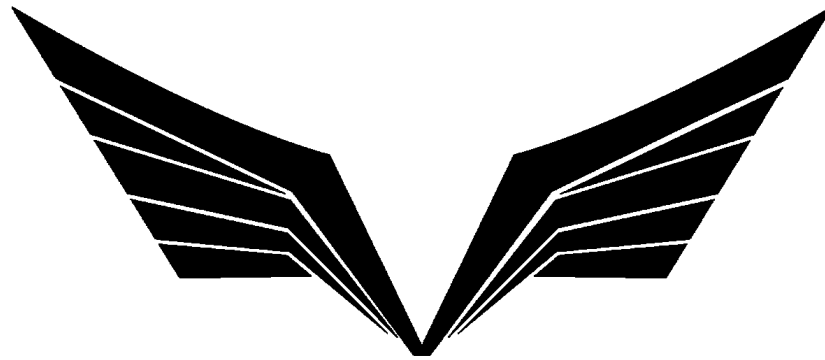




S U N D E V I L

R O C K E T R Y

Avionics Team

New Liquids Feed System (NLFS)
Functional Hazard Assessment (Computer Systems)

Project:	New Liquids Architecture
Author(s)	Eli Sells
Project SQA	Eli Sells, Isahi Soria
Project Lead(s)	Aaron Tsang, Isahi Soria, Eli Sells
Avionics Lead(s)	Eli Sells

TABLE OF CONTENTS

1. COMPONENT BREAKDOWN.....	3
2. FUNCTIONAL HAZARD ANALYSIS.....	5
2.1. HARDWARE COMPONENTS.....	5
2.1.1. LABJACK T7.....	5
2.1.2. GROUND STATION.....	6
2.2. HARDWARE INTERFACES.....	7
2.2.1. LQD-DAQ.....	7
2.2.2. SDEC + SDEC-API.....	8
2.3. USER INTERFACES.....	9
2.3.1. LIQUIDS DASHBOARD.....	9
2.3.2. FLIGHT DASHBOARD.....	10
2.4. NETWORK INTERFACES.....	10
3. SECURITY ANALYSIS.....	11
3.1. DATA FLOWS.....	13
3.1.1. GROUND STATION.....	13
3.1.2. LABJACK.....	14
3.2. NETWORK INTERFACES.....	14
4. COMPONENT LEVEL SQA.....	16
4.1. FLIGHT & LIQUIDS DASHBOARDS.....	16
4.2. LQD-DAQ.....	16
4.3. SDEC + SDEC-API.....	16
4.4. GROUND STATION.....	16
4.5. FULL SYSTEM.....	17
5. ACCEPTABLE FAILURE POINTS.....	18
6. REVISION HISTORY.....	19

1. COMPONENT BREAKDOWN

The feed system's DAQ and control apparatus is a distributed system that is broken down into discrete components. The components are broken down as follows:

1. User Interfaces
 - a. Flight Dashboard
 - b. Liquids Dashboard
2. Hardware Interfaces
 - a. SDEC-API + SDEC
 - b. LQD-DAQ
3. Hardware
 - a. Ground Station
 - b. LabJack T7
4. Network Interfaces
 - a. Layer 3 network interface like a router or managed switch

Each of these components (with the exception of SDEC-API + SDEC) are designed to be able to run on separate computers OR a single device if performance allows (with the exception of the Ground Station and LabJack, which are hardware devices). Most of these components are connected via a socket or HTTP connection, which enables this flexibility. See Figure 1 for a breakdown of these components.

The default/designed launch configuration features four computers. In order of desired system performance/reliability (highest to lowest):

1. Serves the LQD-DAQ server and runs the liquids dashboard.
2. Serves the SDEC-API server, connects the ground station, and runs the flight dashboard.
3. Serves the liquids dashboard and runs an instance of it.
4. Serves the flight dashboard and runs an instance of it.

Additional clients can be connected to run instances of each dashboard. The justification for this prioritization scheme is provided in section 2.

The system boundary is considered to include all of the above components. The system is designed to take inputs/outputs from the user interfaces (within the system boundary) and from

two data flows into the LabJack and Ground Station. Incidental flows are expected from the devices running the system as well as the network interfaces. These incidental flows are not part of the system and mitigations will be provided in this assessment.

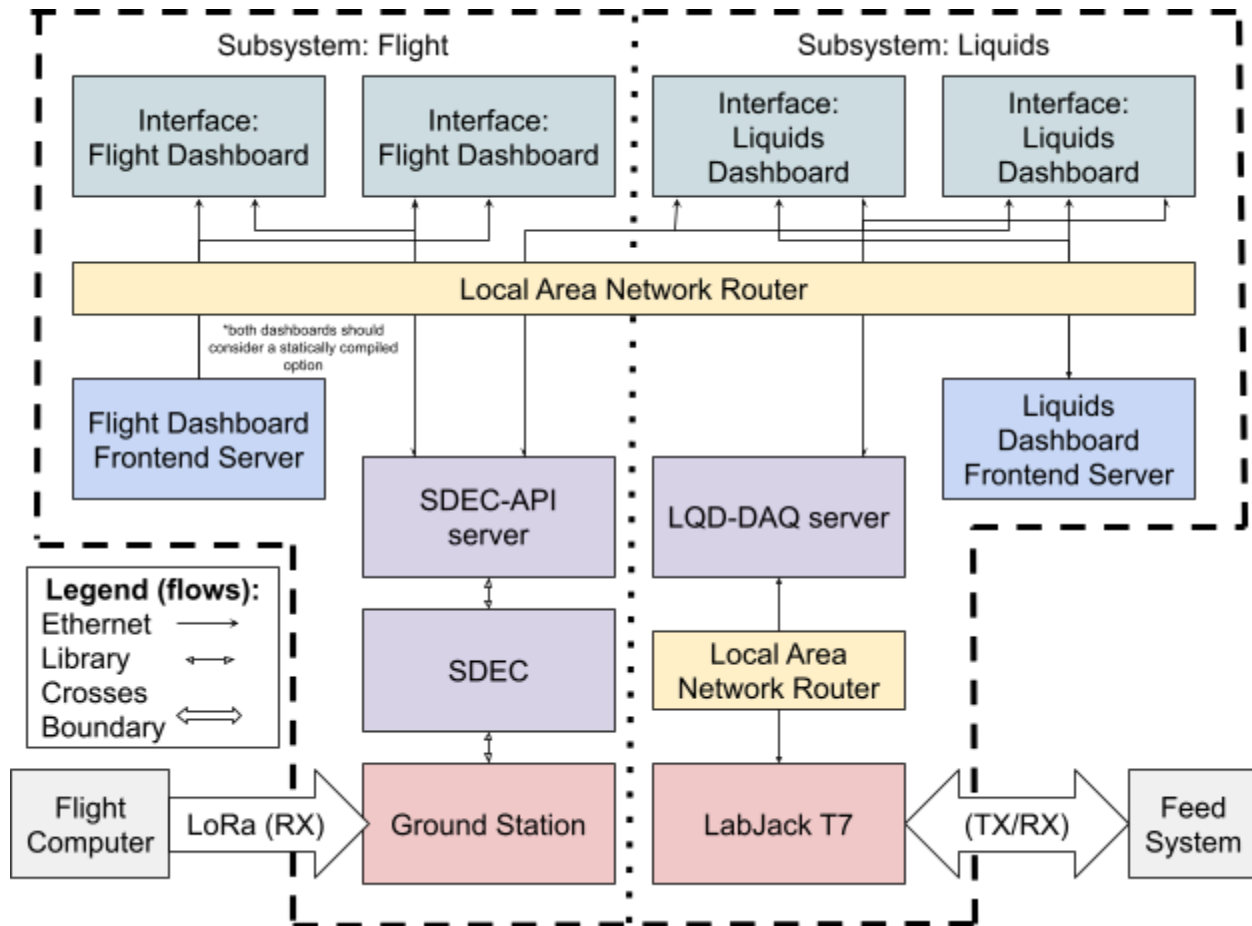


Figure 1: System Boundary

2. FUNCTIONAL HAZARD ANALYSIS

This section will provide component level hazard analyses. See [NLFS FHA Failure Codes](#) for a list of failure codes that can be cross-referenced in source code and other documents.

This analysis is being performed at the system design level. Additional mitigations may be required at component or component integration level. Component integration concerns should consider adding a failure code and revising this document.

2.1. HARDWARE COMPONENTS

2.1.1. LABJACK T7

The LabJack T7 is the feed system's primary source of input data for the liquids subsystem. It also provides control outputs to the feed system to actuate valves. It is designed to be controlled by the LQD-DAQ service and to serve data at a high rate to be logged by the system. This makes the LabJack both *safety and mission critical*.

As a COTS device, internal system errors are considered to be out of scope, but errors in relation to the rest of the system should be handled properly. The following failure modes are known for the LabJack:

Loss of Power (FC.NLFS.LJ.1) is the case where the LabJack and/or other components lose power during the test. The following mitigations should be implemented:

1. Solenoids/valves should be chosen in such a way that the system returns itself to a safe state on loss of power. For example, a vent valve should be normally open if it is expected to vent propellant in the case of an abort scenario.

Loss of LabJack Connection (FC.NLFS.LJ.2) is the case where the LabJack loses its connection to the rest of the system. The following mitigations should be implemented:

1. The LabJack's watchdog timer should be enabled and properly configured. Upon loss of power, the system should return to a safe state.

2.1.2. GROUND STATION

The Ground Station is the primary source of input data for the flight subsystem. It does not provide any control outputs to the system. The Flight Computer ecosystem is designed to run

autonomously after being armed externally, and does not require the Ground Station to operate safely and reliably.

The Ground Station is the primary source of data from sensors on board the rocket. Among these are two pressure transducers used to measure tank pressure. This makes operation of the Ground Station whilst on the ground *safety and mission critical*.

The remaining sensors will only provide useful data in-flight. As their data will be logged internally and any abnormal readings can not be acted upon via control inputs, continued operation of the Ground Station after launch is not safety critical, but should be considered *mission critical*.

Two failure modes are evident for the ground station:

Loss of Ground Station Data (FC.NLFS.GS.1) is the case where the Ground Station stops either receiving or relaying data. This can occur due to failures of the Ground Station, the Flight Computer, or due to the radio environment. Mitigations should be implemented as follows:

1. If the vehicle is on the ground in an unsafe state, an ABORT should be issued. This can be done either automatically or by a human operator.
2. If the vehicle is on the ground in a safe state, a HOLD should be issued. This should be done by a human operator while the issue is triaged by Avionics technicians.
3. If the vehicle is in the air, no further action should be taken.

Misleading Ground Station Data (Benign) (FC.NLFS.GS.2) is the case where the Ground Station receives malformed data from the flight computer due to radio issues. The data transmitted by the Flight Computer is considered trusted, but may be mutated in transit due to malicious or benign reasons. The malicious case is addressed in section 3 as it is a security issue. The benign case can be resolved via the following mitigation:

1. If the received message has a mismatched checksum, discard it and do not relay to SDEC. This defers the case to the mitigations implemented for FC.NLFS.GS.1.

2.2. HARDWARE INTERFACES

2.2.1. LQD-DAQ

LQD-DAQ is the hardware interface layer for the LabJack T7. It reads data from the LabJack, computes derived readings, logs them, and serves the data to the interface. It has a similar

architecture to SDEC-API but has been developed completely independently. Its operation should be considered *safety and mission critical*.

The following failure modes are expected:

Loss of DAQ Background Processing Task (FC.NLFS.LQDDAQ.1) is the case where the background processing engine fails to retrieve data from the LabJack, whether that be due to a downstream issue or because the task crashes from an unrecoverable error. Because of the architecture of LQD-DAQ, it is hard to tell when new data is no longer being received. This should be mitigated via the following:

1. Implement a new heartbeat/watchdog system that requires data to be under a certain age before serving it to the client. If this timeout is expired, provide an indication to the client.

Loss of DAQ Foreground Processing Task (FC.NLFS.LQDDAQ.2) is the case where the foreground task (or the whole system) fails and clients are no longer able to retrieve data. This should be mitigated via the following:

1. If an upstream user that polls LQD-DAQ loses connection, this status should be clearly displayed to the user.
2. If LQD-DAQ no longer has any valid clients, the system should automatically trigger an ABORT.

Rate Throttling of DAQ Foreground Processing Task (FC.NLFS.LQDDAQ.3) is the case where the foreground task receives more requests than it can handle in a reasonable time frame. This should be mitigated via the following:

1. If throttling is detected, clients should be rate limited by the server, except for the /safe and /abort routes.

Loss of Data Logging (LQD-DAQ) (FC.NLFS.LQDDAQ.4) is the case where the DAQ service fails to log the required engine data. Unlike the other failure modes, this affects mission success but has no effect on safety margins. This should be mitigated via the following:

1. An error should be propagated to a status endpoint if data logging fails. Clients should intermittently read this status endpoint and report if the failure is present OR the server should push an error message over the event stream.

Failure to Provide Control Input (LOD-DAQ) (FC.NLFS.LQDDAQ.5) is the case where the DAQ service fails to send a control input properly. This should be mitigated via the following:

1. An error should be propagated to a status input and/or a failure status should be returned from the control endpoint. An abort should be strongly considered in this case.

2.2.2. SDEC + SDEC-API

SDEC and SDEC-API make up the hardware interface layer for the flight subsystem. The two components work together to provide the flight platform's data to the user interface. SDEC is the library that sits on the hardware side and provides interfaces to communicate with the ground station. SDEC-API is the application that integrates with this library. Its background processing loop polls the Ground Station at a steady rate for new data, decoupling the rate of data retrieval from the API layer. The API layer allows the flight and liquids dashboards to fetch the most recently retrieved data from the flight platform.

SDEC and SDEC-API are downstream of the Ground Station and are responsible for mitigating FC.NLFS.GS.1. As these components are responsible for sending safety-critical data to the interfaces for display, their operation should be considered *safety and mission critical*.

The following failure modes are evident for SDEC + SDEC-API:

Loss of SDEC Background Processing Task (FC.NLFS.SDEC.1) is the case where the background processing loop fails to retrieve data from the ground station, whether that be due to a downstream issue or because the task crashes from an unrecoverable error. Because of the architecture of SDEC-API, it is hard to tell when new data is no longer being received. This should be mitigated via the following:

1. Implement a new heartbeat/watchdog system that requires data to be under a certain age before serving it to the client. If this timeout is expired, return a 500 INTERNAL SERVER ERROR status.

Loss of SDEC Foreground Processing Task (FC.NLFS.SDEC.2) is the case where the foreground task (or the whole system) fails and clients are no longer able to retrieve data. This should be mitigated via the following:

1. If an upstream user that polls SDEC loses connection, this status should be clearly displayed to the user.
2. If the vehicle is on the ground in an unsafe state, an ABORT should be issued by the operator (by providing an error message).

3. If the vehicle is on the ground in a safe state, a HOLD should be issued by the operator (by providing an error message).

Rate Throttling of SDEC Foreground Processing Task (FC.NLFS.SDEC.3) is the case where the foreground task receives more requests than it can handle in a reasonable time frame. This should be mitigated via the following:

1. If throttling is detected, clients should be rate limited by the server.

2.3. USER INTERFACES

2.3.1. LIQUIDS DASHBOARD

The liquids dashboard is used to monitor the status of the liquids feed system. It polls SDEC-API for data from the flight platform and LQD-DAQ for data from the liquids platform. It also provides command and control inputs to LQD-DAQ to relay to the LabJack T7. Operation of this interface is both *safety and mission critical*.

The following failure modes are evident for the liquids dashboard:

Loss of SDEC Data (Liquids) (FC.NLFS.LD.1) is the case where the dashboard stops receiving data from SDEC-API. This should be mitigated via the following:

1. If a timeout since the last data response expires, the dashboard should display an indication to the user (complies with FC.NLFS.SDEC.2).
2. If a 500 error is received from a data retrieval endpoint, an indication should be displayed to the user (complies with FC.NLFS.SDEC.1).
3. If the connection fails entirely, the dashboard should show as disconnected from the API (FC.NLFS.SDEC.2).

Loss of Liquids Data (FC.NLFS.LD.2) is the case where the dashboard stops receiving data from LQD-DAQ. This should be mitigated via the following:

1. If a timeout since the last data response expires, the dashboard should display an indication to the user (complies with FC.NLFS.LQDDAQ.2).
2. If a 500 error is received from a data retrieval endpoint, an indication should be displayed to the user recommending an ABORT (complies with FC.NLFS.LQDDAQ.1).
3. If the connection fails entirely, the dashboard should show as disconnected from the API (complies with FC.NLFS.LQDDAQ.2).

Loss of Command/Control (FC.NLFS.LD.3) is the case where the dashboard is unable to provide control inputs to the LabJack via LQD-DAQ. This should be mitigated via the following.

1. An indication should be presented to the user recommending the system be aborted manually.

2.3.2. FLIGHT DASHBOARD

The flight dashboard is used to monitor the status of the flight avionics platform. It polls SDEC-API for flight data and uses this to update GPS position, altitude, and orientation readouts. As the flight ecosystem does not take command inputs after arming, operation of the flight dashboard during any phase of flight is to be considered neither safety nor mission critical.

Nonetheless, it is still useful to be able to receive data from this platform. The following failure modes are expected for the flight dashboard:

Loss of Dashboard Data (FC.NLFS.FD.1) is the case where the dashboard stops receiving data from SDEC-API. This should be mitigated via the following:

1. If a timeout since the last data response expires, the dashboard should display an indication to the user (complies with FC.NLFS.SDEC.2).
2. If a 500 error is received from a data retrieval endpoint, an indication should be displayed to the user (complies with FC.NLFS.SDEC.1).
3. If the connection fails entirely, the dashboard should show as disconnected from the API (FC.NLFS.SDEC.2).

2.4. NETWORK INTERFACES

The network interfaces used in the system shall be COTS (commercial off the shelf) products with a proven high degree of reliability. As such, internal errors with the network interfaces are considered to be out of scope for the purposes of this assessment. For security analysis, see section 3.

3. SECURITY ANALYSIS

Security risks to this device will be scored via the same methods as the Flight Computer: a matrix that accounts for likelihood and severity.

Table 1: Likelihood Scores

Likelihood Score	Description
L0	No possibility of access to the system
L1	Complex attack vector requiring physical access to equipment
L2	Simple attack vector requiring physical access to equipment
L3	Complex attack vector that can be executed remotely
L4	Simple attack vector that can be executed remotely

Table 2: Severity Scores

Severity Score	Description
S0	No effects on the system
S1	Effects are limited to minor subsystems
S2	Causes an unrecoverable error
S3	Impacts data served to the operator
S4	Allows malicious control inputs

The likelihood scores are biased towards remote access attacks. These are considered more likely as they can be exploited without the user's knowledge regardless of access control to the physical device.

Unrecoverable errors are given a severity score of 2 because there are scenarios on this system where it is preferable to do nothing than to take the wrong action due to the mitigations

implemented at the LabJack hardware level. An attacker having control over control systems is considered the worst-case scenario.

A composite score shall be created from these two factors to describe the mitigation strategies that should be taken for each scenario.

Table 3: Threat Scores

Threat Score	Description	Mitigation Strategies
T0	Not considered for security purposes	No mitigation required
T1	Minor Threat	Dependency analysis, standard code review
T2	Moderate Threat	Dependency analysis, standard code review, single weak or greater security measure
T3	Major Threat	Dependency analysis, security expert code review, single strong security measure
T4	Catastrophic Threat	Dependency analysis, security expert code review, dual & dissimilar security measures (at least one strong measure)

From these tables above, threat scenarios will be scored on a scale of 0-4 according to the following matrix:

Table 4: Threat Level Matrix

\	L0	L1	L2	L3	L4
S0	T0	T0	T0	T0	T0
S1	T0	T1	T1	T2	T2
S2	T0	T1	T1	T3	T3
S3	T0	T1	T1	T4	T4
S4	T0	T1	T2	T4	T4

3.1. DATA FLOWS

This section discusses attack vectors related to data that is expected to cross the system boundary during normal operation.

3.1.1. GROUND STATION

The Ground Station's data flow is a one-way reception of data from the Flight Computer over LoRa. The Flight Computer and the data it sends are considered to be trusted, but the method of transmission is not. Thus, there exists an attack vector to inject misleading data to the liquids system by transmitting to the Ground Station. As-is, the system will reject incoming data on the chosen frequency that is encoded with the wrong bandwidth, spreading factor, error coding rate, or that fails a cyclic redundancy check (CRC). Thus, if the frequency is already in use, the threat is mitigated by existing methods (see FC.NLFS.GS.2).

However, this does not account for malicious actors. If an actor was intentionally attempting to compromise the system, they would likely be able to match all of these parameters in order to feed malicious data.

Misleading Ground Station Data (Malicious) (FC.NLFS.GS.3) is the case where the Ground Station receives malformed data from the flight computer due to an outside actor intentionally trying to hinder operations of the system. The data transmitted by the Flight Computer is considered trusted, but may be mutated in transit due to malicious or benign reasons. The benign case is addressed in section 2. This case is scored with the following severity:

- Likelihood: L4 (requires specialized equipment, but does not require a network or software level compromise to exploit).
- Severity: S3 (serves misleading data to operator)
- Threat score: T4

This case can be resolved via the following mitigation:

1. If the received message has a mismatched signature or does not decode properly, discard it and do not relay to SDEC. The signature or encryption shall be considered the strong security measure, and the CRC check is a dual & dissimilar measure. This defers the case to the mitigations implemented for FC.NLFS.GS.1.

3.1.2. LABJACK

The LabJack T7 is a COTS device that will only take inputs from physically accessible interfaces or the wired network. Access control is deferred to the network interfaces section of this analysis. Sensor tampering requires physical access immediately after deployment of the system within the controlled zone, and is considered out of scope.

3.2. NETWORK INTERFACES

The network interfaces used to connect the system's components are arguably the riskiest attack vector available to the system. Any compromise of network security would allow total control of the system with very little difficulty. There are two general routes to accomplish this:

Wireless Network Access Control Failure (FC.NLFS.NI.1) describes the case where an unauthorized user gains access to the local area wireless network used to connect the components of the system. This case is scored with the following severity:

- Likelihood: L3 (requires guessing or brute-forcing a password – a weak password is expected pre-mitigation)
- Severity: S4 (total system compromise)
- Threat score: T4

This case can be resolved via the following mitigations:

1. If the router in use is wireless capable, the firmware should be up to date AND no more than one year old to mitigate known vulnerabilities.
2. The router shall employ a “strong” password (xref: [CISA](#)); (the strong method).
3. The router shall employ a form of brute force prevention to lock out repeated attempts (the dual/dissimilar method).
4. Dependency analysis, security expert code review

Wired Network Access Control Failure (FC.NLFS.NI.2) describes the case where an unauthorized user gains access to the local area wired network used to connect the components of the system. This case is scored with the following severity:

- Likelihood: L2 (no password in use, but physical access required)
- Severity: S4 (total system compromise)
- Threat score: T2

This case can be resolved via the following mitigations:

1. Physical access to the system shall be controlled (weak measure).
2. Dependency analysis, standard code review

4. COMPONENT LEVEL SQA

Each component has agreed to the following SQA practices to ensure reliability.

4.1. FLIGHT & LIQUIDS DASHBOARDS

The dashboards (Software Division) will employ the following practices:

- Code reviews required for all functional changes
 - A baseline will be established with a full-app review, then reviews required for every incoming PR
- Regular scanning for issues/vulnerabilities in dependencies
- Structured release schedule with system testing

4.2. LQD-DAQ

The LQD-DAQ service will employ the following practices:

- Code reviews required for all functional changes
 - A baseline will be established with a full-app review, then reviews required for every incoming PR
- Regular scanning for issues/vulnerabilities in dependencies
- Automated testing of major features
- Structured release schedule with system testing

4.3. SDEC + SDEC-API

SDEC and SDEC-API will employ the following practices:

- Code reviews required for all functional changes
 - Reviews are required for every PR since baseline tag v2.0.0
- Regular scanning for issues/vulnerabilities in dependencies
- SDEC: Automated testing of major features
- Structured release schedule with system testing

4.4. GROUND STATION

The Ground Station will employ the following practices:

- Code reviews required for all functional changes
 - A baseline will be established with a full-app review, then reviews required for every incoming PR

- Structured release schedule with system testing

4.5. FULL SYSTEM

The system as a whole will employ the following practices:

- Intermittent SQA audits of component level compliance.
- An integration period of at least two weeks should be provided before the first launch or hot-fire test.
- System testing upon component releases

5. ACCEPTABLE FAILURE POINTS

Based on the hazard analysis, some components are able to be non-functional without harming the integrity of the test at certain points. At each of the following GO/NO-GO points, the components are permitted to have the following failures present. If any failures are present that ARE NOT listed here, the test should be held or aborted.

1. Test Start (all test stand avionics powered on; flight avionics not powered on)
 - a. All systems must be operational & status nominal
2. Pre-fill Purge GO/NO-GO
 - a. All systems must be operational & status nominal
3. Propellant Fill GO/NO-GO (Flight platform will power & arm prior to LOX fill)
 - a. Flight Dashboard - Any failure permitted **IF AND ONLY IF** liquids dashboard is receiving onboard data
4. Tank Pressurization GO/NO-GO
 - a. Flight Dashboard - Any failure permitted **IF AND ONLY IF** liquids dashboard is receiving onboard data

6. REVISION HISTORY

1.0 - Initial Revision

APPENDIX A. DEFINITIONS

TERM	DEFINITION
LQD-DAQ	LQD-DAQ (pronounced “liquid dack”) is an application that exposes certain utilities over HTTP (hypertext transfer protocol) to enable networked applications to interact with a connected LabJack T7. This enables a web-based user interface to display data and send commands to the T7, even from another computer.
SDEC	SDEC stands for Sun Devil Embedded Control. It is the primary software library used by the Avionics Firmware team to send commands to and retrieve data from embedded computers in use by the club.
SDEC-API	SDEC-API is an application built around the SDEC library. It exposes certain utilities provided by the library over HTTP (hypertext transfer protocol) to enable networked applications to interact with a connected embedded computer. Its primary use (prior to development of the New Liquid Feed System) is to serve flight data from a live telemetry source to the Flight Dashboard.