

# Detecting and Characterizing Patterns of Failure in Complex Systems: An Ontology Development and Clustering Approach



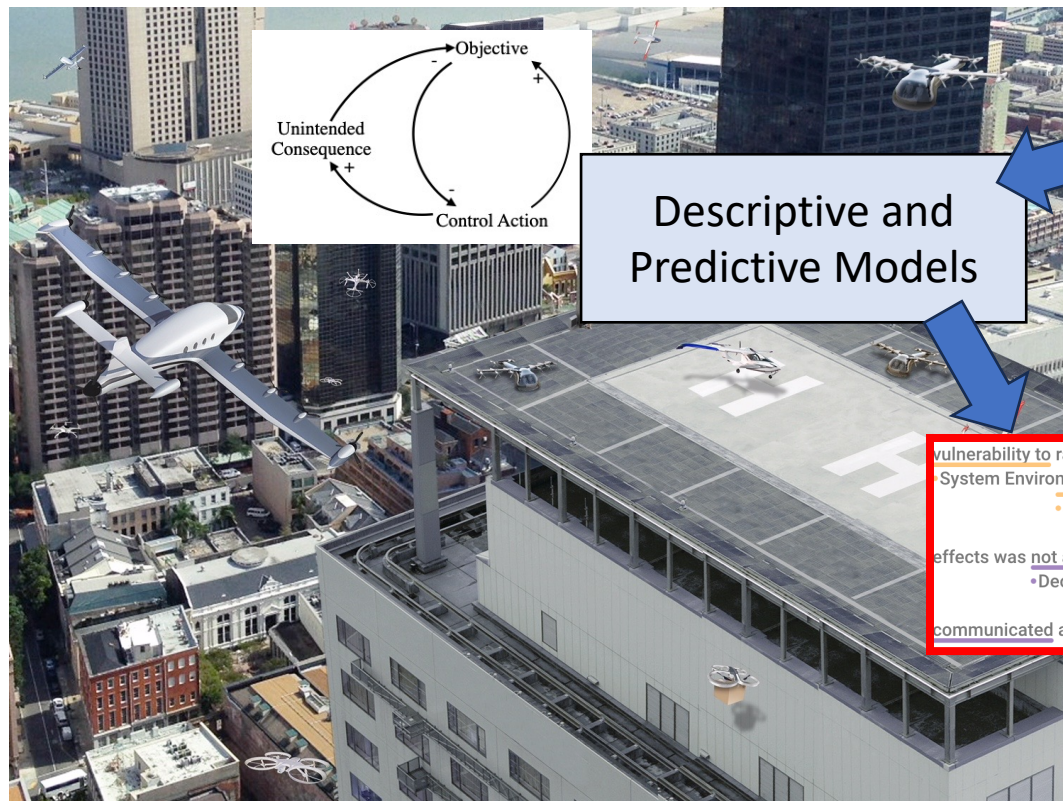
ICED23  
24-28 July 2023

Hannah Walsh, **Andy Dong**, Irem Tumer, and Guillaume Brat

# Introduction

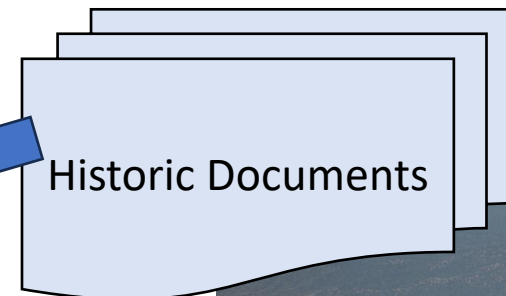


## New System



[images-assets.nasa.gov/image/UAM/UAM~orig.jpg](https://images-assets.nasa.gov/image/UAM/UAM~orig.jpg)

## Current/Past Systems



[images-assets.nasa.gov/image/EC05-0148-30/EC05-0148-30~orig.jpg](https://images-assets.nasa.gov/image/EC05-0148-30/EC05-0148-30~orig.jpg)

vulnerability to radiation  
System Environment: Interaction with Environment  
• System Environment: Interaction with Environment  
effects was not adequately  
• Decision-Making Structure: Too Centralized  
communicated across the MSL

## Lesson Info

|                         |            |
|-------------------------|------------|
| Lesson Number           | 1710       |
| Lesson Date             | 2003-07-03 |
| Submitting Organization | LARC       |

Labeling scheme:

Problem

Asset

Solution

(Brundage et al, 2021)

## Subject

*Uninhabited Aerial Vehicle (UAV), Flight Test Operations, Accident Investigation*

## Abstract

A high performance jet-powered UAV crashed on landing. A subsequent investigation into the root cause(s) found that the ground support crew did not follow all of the steps in a complex checklist and the pilot did not adhere to the flight parameters dictated by the flight test card. Omission of pre-flight steps resulted in lower than expected engine thrust performance. This off-nominal thrust condition caused the pilot to attempt to compensate throughout the flight. This compensation, along with other complicating factors, caused the pilot to mismanage the UAV's energy, resulting in a landing touchdown speed that was well above rated touchdown speed, resulting in the collapse of the left main landing gear. The pilot did not have any previous experience with this UAV. A primary complicating factor was that the pilot did not know and was not briefed on several key UAV performance factors, primary of which was maximum touchdown speed. Less than adequate communications between the pilot and ground support crew both in pre-flight and flight was also a complicating factor. During the crash, the flight crew was exposed to potential injury since they were situated at the runway edge near the UAV touchdown point.

Execution of each step in a checklist should be independently verified, especially the complex checklists used in these operations. A pilot briefing on critical vehicle performance parameters should be given even if the pilot is expected to know critical flight parameters. Communications between pilot and ground support crew should be full and open during preflight and flight. Real time warnings should be provided to the pilot when deviating from the planned flight test parameters. The flight crew should maintain a safety barrier device between themselves and the vehicle during the landing sequence.

## Lesson Info

|                         |            |
|-------------------------|------------|
| Lesson Number           | 1710       |
| Lesson Date             | 2003-07-03 |
| Submitting Organization | LARC       |

Labeling scheme:

Procedures

Decision-Making Structure

Human-System Relationship

(This work)

## Subject

*Uninhabited Aerial Vehicle (UAV), Flight Test Operations, Accident Investigation*

## Abstract

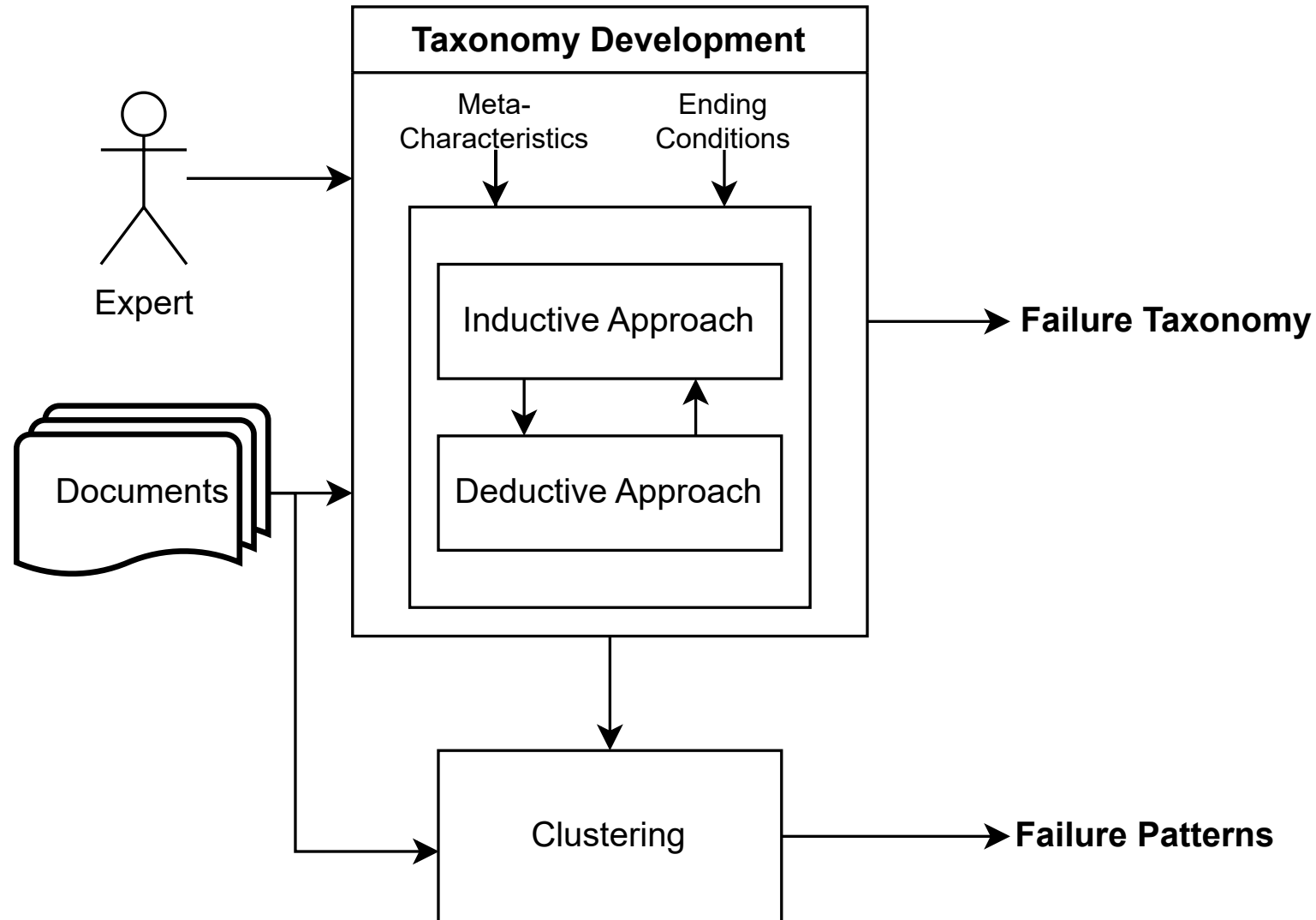
A high performance jet-powered UAV crashed on landing. A subsequent investigation into the root cause(s) found that the ground support crew did not follow all of the steps in a complex checklist and the pilot did not adhere to the flight parameters dictated by the flight test card. Omission of pre-flight steps resulted in lower than expected engine thrust performance. This off-nominal thrust condition caused the pilot to attempt to compensate throughout the flight. This compensation, along with other complicating factors, caused the pilot to mismanage the UAV's energy, resulting in a landing touchdown speed that was well above rated touchdown speed, resulting in the collapse of the left main landing gear. The pilot did not have any previous experience with this UAV. A primary complicating factor was that the pilot did not know and was not briefed on several key UAV performance factors, primary of which was maximum touchdown speed. Less than adequate communications between the pilot and ground support crew both in pre-flight and flight was also a complicating factor. During the crash, the flight crew was exposed to potential injury since they were situated at the runway edge near the UAV touchdown point.

Execution of each step in a checklist should be independently verified, especially the complex checklists used in these operations. A pilot briefing on critical vehicle performance parameters should be given even if the pilot is expected to know critical flight parameters. Communications between pilot and ground support crew should be full and open during preflight and flight. Real time warnings should be provided to the pilot when deviating from the planned flight test parameters. The flight crew should maintain a safety barrier device between themselves and the vehicle during the landing sequence.

- **The bottom line: we need a labeling scheme that is appropriate for the specific use**
  - However, the scheme must also be (1) logical and (2) representative of the content it will be used to label
- **For this purpose, we propose the systematic development of a taxonomy to guide annotation**
  - The taxonomy can also be used for descriptive studies of the set of documents, such as finding patterns of failure

- **Labeling for natural language processing tasks**
  - Developing ontologies (Wang et al, 2021, and Ye et al, 2016)
  - FMEA-style labels (Andrade & Walsh, 2022)
- **Ontologies of design knowledge**
  - Taxonomy of error types (Sutcliffe & Rugg, 1998)
  - Ontologies used for information retrieval (Li et al, 2014)
- **Identifying patterns in ontological characteristics**
  - Archetypal blockchain business models (Weking et al, 2020)
  - Platform envelopment (Hermes et al, 2020)

# Methodology Overview



# NASA Lessons Learned Information System



## Subject

*Thermal Control System (TCS) Blanket Interference with Xo378 Bulkhead Vent Ports [Video Lesson]*

## Abstract

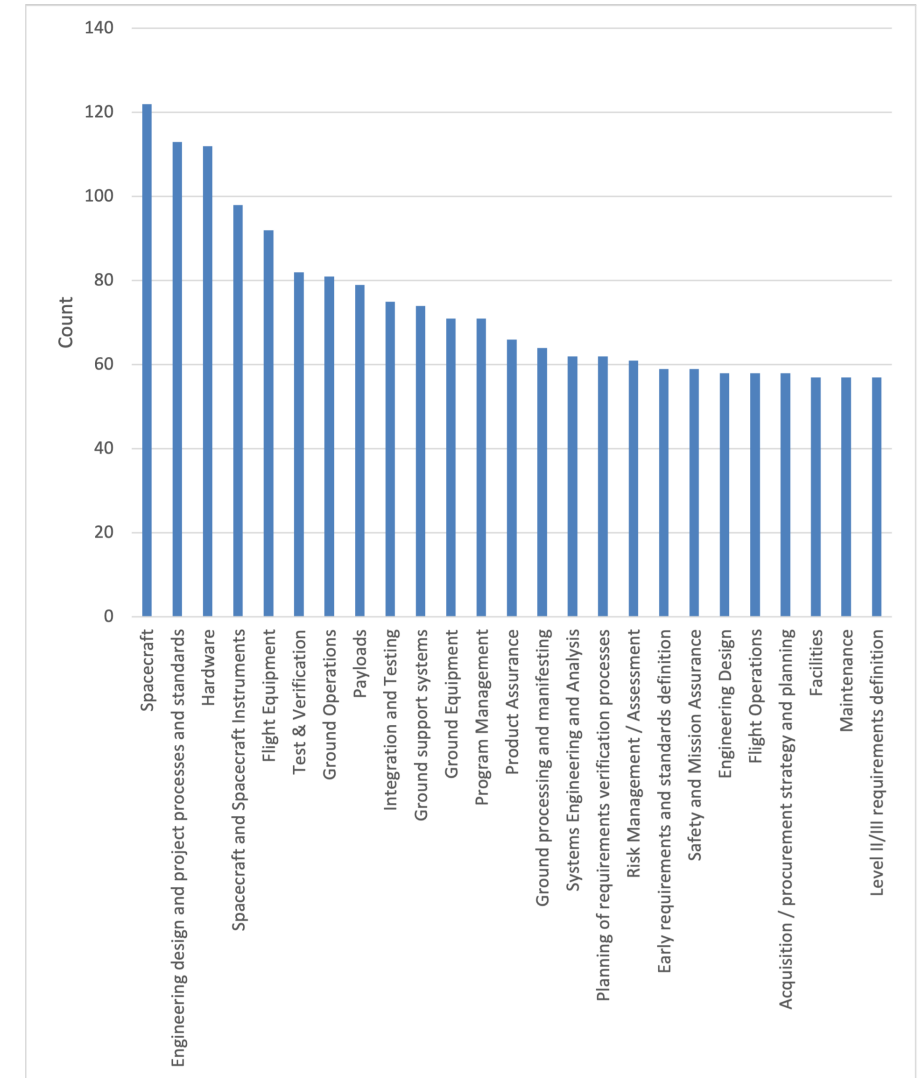
TCS blankets by nature have a close and critical dimensional relationship to the surrounding hardware they are insulating. Blankets were installed incorrectly over the Purge Vent Drain (PVD) lines in the Forward Reaction Control System (FRCS). Incorrect installation allowed the blankets to billow toward the Xo 378 bulkhead vents, restricting venting of the FRCS cavity.

## Driving Event

During STS-121 ascent, the Xo 378 bulkhead delta-pressure transducer showed higher than normal pressure differential across the bulkhead. Following the STS-121, ground borescope inspections on FRC3 showed that TCS blankets in the FRCS module were very close to the vents, and were not installed under the Purge Vent Drain (PVD) lines. Design intent is to install the V070-361995-024 Left Hand (LH) and V070-361995-025 Right Hand (RH) Multilayer Insulated blankets (MLI) under PVD drain lines in the FRCS. The blankets contain existing cutouts and cutlines, allowing installation under these lines. When properly installed, the blankets are restrained by the PVD drain lines and cannot billow into the Xo 378 vent areas. Using templates to simulate a Xo378 vent port, TCS Engineering determined that blockage of the vent ports can occur when blankets are installed on top of the drain lines. Improper installation of the TCS blankets was determined to be the cause of the vent anomaly.

## Lesson(s) Learned

The interface between TCS blankets and their associated hardware needs to be clearly and unambiguously documented on the installation drawings so that blankets perform as designed without unintended interferences or blockages particularly related to cutouts and openings. System operators need to understand how all the pieces fit together so that each team member appreciates how their contribution affects the integrated system.



# Taxonomy Development



- **Define Meta-characteristics and Ending Conditions to begin**
- **Alternate between Inductive and Deductive Approach until Ending Conditions are met**
  - Can start with either Inductive or Deductive Approach, depending on familiarity with the database
  - Entire set of documents is used for each iteration
- **Taxonomy in this approach is a set of dimensions and characteristics**
  - Multiple characteristics belong to one dimension
  - Characteristics are a logical consequence of meta-characteristic and do not apply to all documents
  - Characteristics in each dimension are mutually exclusive
  - Dimensions are collectively exhaustive

# Meta-Characteristic and Ending Conditions



- **Meta-Characteristic**

- Consider taxonomy purpose and targeted characteristics
- Meta-characteristics: characteristics of the system architecture, operation, environment, or development process that introduce a hazard

- **Ending Conditions**

- After each iteration (inductive + deductive), check whether ending conditions are met
  - Yes: taxonomy is complete
  - No: continue iterating
- Standard ending conditions:
  - Mutually exclusive and collectively exhaustive
  - All documents (or a representative sample) have been analyzed
  - No merges, splits, or new characteristics in most recent iteration
  - Each characteristic is described in at least one document
  - Each dimension and each characteristic within a dimension is unique
  - Each combination of characteristics is unique
- Application-specific ending conditions can also be added

# Inductive & Deductive Approaches



## • Inductive Approach

- Read all documents (or a representative sample) to gain understanding of information
- Highlight parts of text that capture key themes
- Make notes of thoughts and analysis

vulnerability to radiation

- System Environment: Interaction with Environment

- System Environment: Interaction with Environment

effects was not adequately

- Decision-Making Structure: Too Centralized

communicated across the MSL

## • Deductive Approach

- Start by reading characteristics
- Consider whether documents are described by characteristics
- Add, remove, or merge characteristics and dimensions as needed

Characteristics:

**System Environment: Interaction with Environment**

**Decision-Making Structure: Too Centralized**

Document:

Both the Juno and Mars Science Laboratory (MSL) spacecraft experienced anomalies in memory devices due to single event functional interrupts (SEFIs) occurring during the cruise phase of the missions. A known problem potentially affecting other spaceflight projects, the parts' vulnerability to radiation effects was not adequately communicated across the MSL project. Part test results should be more widely communicated, and projects need to be more penetrating in review of known part failure mechanisms.

- **Clustering to find patterns of failure**
- **Patterns of failure: dimensions of failure that tend to appear together in a single document describing a failure**
- **Multiple algorithms tested – spectral clustering performed best for this application**
- **Evaluated using silhouette coefficient**

Silhouette Coefficient:

$$s = \frac{b - a}{\max(a, b)}$$

$a$ : mean intra-cluster distance

$b$ : mean nearest cluster distance

Measured per sample (document).

Average and standard deviation across samples is usually considered.

# Results (1)

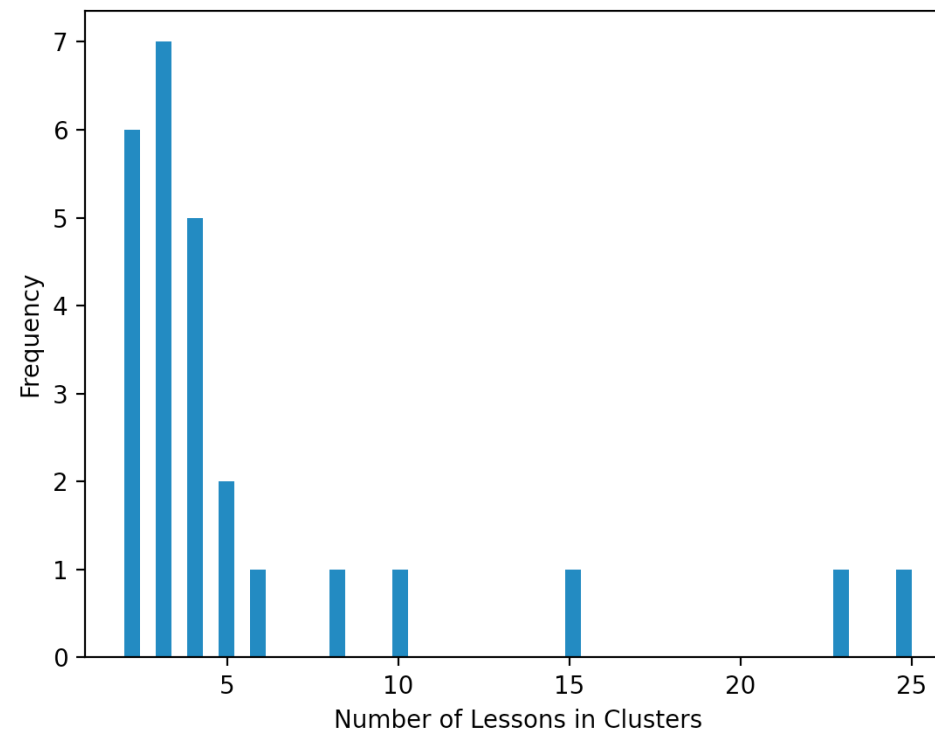


| Dimension                 | Characteristic                                         | Definition                                                                                   | Count |
|---------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------|-------|
| Analysis                  | Development Process Missing Standard Analysis          | An analysis that is widely considered standard is not performed                              | 48    |
|                           | Standard Analysis Not Performed on Final Configuration | Analysis is performed, but too early, so the final configuration is not analyzed             | 16    |
|                           | Analysis is Adequate for System Operation              | Standard analysis is performed at an appropriate time in design                              | 86    |
| Decision-Making Structure | Too Centralized                                        | Single decision-maker does not communicate sufficiently                                      | 23    |
|                           | Too Decentralized                                      | Multiple decision-makers are not well coordinated                                            | 20    |
|                           | Decision-Making Structure is Effective                 | Decision-maker(s) and communications are suited to decision                                  | 107   |
| Human-System Relationship | Inadequate Human Factors                               | Human factors not adequately considered during design                                        | 12    |
|                           | Adequate Human Factors                                 | Human factors adequately considered during design                                            | 138   |
| Monitoring                | Failure of Monitor                                     | Monitor is present, but failed                                                               | 1     |
|                           | Omission of Monitor                                    | Monitor is needed, but not present                                                           | 8     |
|                           | Monitors Adequate and Functional                       | Monitor is either not needed or present and functional                                       | 141   |
| Procedures                | Intrusion or Replacement of Procedure                  | Addition of new procedure or replacement of a correct step with an incorrect step            | 7     |
|                           | Omission of Procedure                                  | Operator skips a step or procedure                                                           | 14    |
|                           | Procedures Adequate and Appropriate                    | Only correct procedures are followed, if any are required                                    | 129   |
| Safety Equipment          | Inadequate Safety Equipment                            | Safety equipment or safeguards are inadequate                                                | 6     |
|                           | Adequate Safety Equipment                              | Safety equipment or safeguards are adequate                                                  | 144   |
| Subsystem Behavior        | Coupling between Subsystems                            | Small deviation in one subsystem affects another subsystem                                   | 30    |
|                           | Isolated Subsystems                                    | Subsystems difficult to integrate                                                            | 8     |
|                           | Subsystem Interaction Effective                        | Subsystem interaction is effective                                                           | 112   |
| System Behavior           | Unaccounted for Non-Linear Behavioral Relationships    | A small deviation or fault has large impacts on system-level behavior                        | 10    |
|                           | Accounted for Behavioral Relationships                 | If non-linear relationships exist, they are accounted for in design or operation             | 140   |
| System Environment        | Unaccounted for Interaction with Environment           | Interactions between the system and its environment are not adequately isolated or protected | 31    |
|                           | Accounted for Interaction with Environment             | Interactions between the system and its environment are adequately isolated or protected     | 119   |
| Timing of Action          | Premature Action                                       | An action in design or operation is made prematurely                                         | 5     |
|                           | Delayed Action                                         | An action in design or operation is made late                                                | 2     |
|                           | Action Timed Appropriately                             | An action in design or operation is made at the correct time, if one is needed               | 13    |

# Results (2)



| No. | Size | Sample Lesson | Characteristics                                                                                                                                                                                                                                                  |
|-----|------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | 25   | 26703         | (1) <b>Analysis:</b> "Knowledge of the 1-g physics of large bubbles in the condenser legs would have allowed the limits of ground testing to be better understood."                                                                                              |
| 2   | 23   | 24503         | (1) <b>Decision-Making Structure:</b> "flight software has been developed by a consortium... The definition of the software coding standards was non-specific."                                                                                                  |
| 3   | 15   | 24403         | (1) <b>System Environment:</b> "Bird Strikes are known hazards during aircraft takeoff and landing operations."                                                                                                                                                  |
| 4   | 9    | 28101         | (1) <b>Analysis:</b> "the redundancy and failure analysis for LRS was incomplete", (2) <b>Subsystem Relationships:</b> "include all relevant interfacing subsystems"                                                                                             |
| 5   | 9    | 27003         | (1) <b>Subsystem Relationships:</b> "have been found to have sensitivity to noise that could lead to inadvertent firing"                                                                                                                                         |
| 6   | 6    | 27701         | (1) <b>Analysis:</b> "robust design practices and integrated set of engineering checks and balances that may have prevented...", (2) <b>System Environment:</b> "radiation-induced damage"                                                                       |
| 7   | 5    | 1710          | (1) <b>Procedures:</b> "did not follow all of the steps in a complex checklist", (2) <b>Decision-Making Structure:</b> "Less than adequate communications between...", (3) <b>Human-System Relationship:</b> "...caused the pilot to mismanage the UAV's energy" |
| 8   | 4    | 28105         | (1) <b>Subsystem Relationships:</b> "propulsion subsystem should ensure positive isolation of..."                                                                                                                                                                |
| 9   | 4    | 4999          | (1) <b>Procedures:</b> "active leveling should be employed to accommodate center of gravity offsets"                                                                                                                                                             |
| 10  | 4    | 28202         | (1) <b>Analysis:</b> "warranted the need to perform a second round of fatigue analysis", (2) <b>Decision-Making Structure:</b> "stress analysis team was not made aware of the change"                                                                           |



Moderate to strong cluster structure  
( $s=0.7704$ )

# Discussion, Conclusions, and Future Work



- **Limited by what contributors include in the LLIS entry**
- **Some overlap when compared to similar, existing taxonomies (e.g., Sutcliffe & Rugg)**
- **Identified twenty-seven patterns of failure and developed a taxonomy for describing twenty-six characteristics grouped into ten dimensions**
  - Results provide a conceptual model for developing a labeling scheme for natural language processing tasks
- **Future work will apply the method to other datasets to test extensibility and improve the breadth of failures characterized**
  - Broader project will require interpretation by SMEs

# Thank you! Questions?

## References:

- Andrade, S. and Walsh, H.S. (2022a), “What went wrong: a survey of wildfire UAS mishaps using named entity recognition”, in: Digital Avionics Systems Conference (DASC).
- Brundage, M., Sexton, T., Hodkiewicz, M., Dima, A., and Lukens, S. (2021) “Technical language processing: Unlocking maintenance knowledge”, *Manufacturing Letters*, Vol. 27, pp. 42-46.
- Hermes, S., Kaufmann-Ludwig, J., Schreieck, M., Weking, J. and Böhm, M. (2020), “A taxonomy of platform envelopment: Revealing patterns and particularities”, *AMCIS 2020 Proceedings*.
- Li, L., Qin, F., Gao, S. and Liu, Y. (2014), “An approach for design rationale retrieval using ontology-aided indexing”, *Journal of Engineering Design*, Vol. 25 No. 7-9, pp. 259–279, 10.1080/09544828.2014.969690
- Sutcliffe, A. and Rugg, G. (1998), “A taxonomy of error types for failure analysis and risk assessment”, *Int. J. Hum. Comput. Interaction*, Vol. 10, pp. 381–405, 10.1207/s15327590ijhc10045.
- Wang, K., Stevens, R., Alachram, H., Li, Y., Soldatova, L., King, R., Ananiadou, S., Schoene, A.M., Li, M., Christopoulou, F. et al. (2021), “Nero: a biomedical named-entity (recognition) ontology with a large, annotated corpus reveals meaningful associations through text embedding”, *NPJ systems biology and applications*, Vol. 7 No. 1, pp. 1–8.
- Weking, J., Mandalenakis, M., Hein, A., Hermes, S., Böhm, M. and Krcmar, H. (2020), “The impact of blockchain technology on business models — a taxonomy and archetypal patterns”, *Electronic Markets*, Vol. 30, p. 285–305, 10.1007/s12525-019-00386-3.
- Ye, D., Xing, Z., Foo, C.Y., Ang, Z.Q., Li, J. and Kapre, N. (2016), “Software-specific named entity recognition in software engineering social content”, in: 2016 IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER), Vol. 1, pp. 90–101, 10.1109/SANER.2016.10.

