DANGEROUS GOODS PANEL (DGP)

TWENTY-NINTH MEETING

Montréal, 13 to 17 November 2023

Agenda Item 4: Managing safety risks posed by the carriage of lithium batteries by air *(Ref: Job Card DGP.003.04)*

REPORT OF THE DANGEROUS GOODS PANEL WORKING GROUP ON ENERGY STORAGE DEVICES (DGP-WG/ENERGY STORAGE DEVICES): SYSTEMS THEORETIC PROCESS ANALYSIS (STPA)

(Presented by the Rapporteur of DGP-WG/Energy Storage Devices)

SUMMARY

This information paper contains a report developed by DGP-WG/Energy Storage Devices applying Systems Theoretic Process Analysis to the air transport of lithium ion batteries packed with or contained in equipment.

1. INTRODUCTION

1.1 The twenty-eighth meeting of the Dangerous Goods Panel (DGP/28, 15 to 19 November 2021) requested the DGP Working Group on Energy Storage Devices (DGP-WG/Energy Storage Devices) to conduct a safety risk assessment on lithium batteries packed with or contained in equipment and vehicles under the guidance of ICAO safety management experts. The working group applied Systems Theoretic Process Analysis (STPA) to explore the hazards associated with the air transport of UN 3481 lithium ion batteries packed with equipment and lithium ion batteries contained in equipment. Existing safety requirements and potential new requirements were assessed against a mitigation order of precedence scale. Lithium ion batteries packed with and contained in equipment were selected for this analysis because these configurations have similar characteristics and requirements while lithium ion battery powered vehicles comprise a broad range of products and sizes that may warrant special consideration.

1.2 The aim of the attached report is to provide an alternate perspective analysis of the hazards associated with the transport of lithium batteries by aircraft. Traditional hazard analysis typically involves dividing the system into components and assuming that accidents/incidents are caused by component failure. The probability of a failure of each component is then calculated separately and later combined. The level of risk is typically defined as a product of severity of an event (e.g. a thermal runaway of lithium ion batteries in an aircraft cargo compartment) and the likelihood of that event or a specific series of events leading to that outcome. This is used to determine whether the risk is sufficiently controlled. This method of risk assessment poses significant challenges when assessing lithium battery thermal runaway events because this method relies upon certain information and assumptions that do not apply here. First, this technique requires detailed data on the system and its components including the number of shipments and packages transported, specifics of the package contents such as whether packages contained only equipment, or equipment and spare batteries, the types of equipment, incident rates, reliable information about the specific cause of the incident, and individual factors that contribute to incidents. Such information is largely unavailable or insufficiently detailed to inform a standard analysis. Lithium battery incidents are low-probability events with outsized consequences and thus the predictability of such events is suspect. Second, it assumes that observations of past behaviour allow accurate prediction of future behaviour. The fast pace of technological change, new system entrants and an evolving regulatory landscape create cases where previous knowledge of system safety is of little benefit in generating probabilities. The STPA method overcomes many of these limitations by emphasizing interactions between system components and identifying ways that interactions violate system constraints. Further, since STPA aims to prevent losses, this type of analysis is not limited to previously identified failures.

1.2.1 The DGP-WG/Energy Storage Devices applied this method to the air transport of lithium ion batteries packed with and contained in equipment and identified several themes:

a) The information presented during previous DGP working group meetings indicates a significant increase in lithium ion battery powered equipment air transport volumes, a demonstrated fire hazard when a lithium ion cell or battery goes into thermal runaway, and incidents with lithium ion cells and batteries in air transport including handling prior to or after air transport (not limited to cargo shipments).

b) The supply chain for lithium ion batteries and equipment is fragmented and has many interactions amongst supply chain participants that introduce the possibility of safety issues.

c) Provisions in the Technical Instructions designed to facilitate transport of lithium ion batteries packed with equipment and lithium batteries contained in equipment (i.e. Packing Instructions 966 and 967) limit the ability of supply chain participants to identify shipments and apply hazard mitigation measures.

d) Civil aviation authorities obtain most of their information on safety performance through incident reports and inspections. As a result, such information is obtained only after losses (e.g. thermal events) and non-compliance with safety requirements have been observed.

e) Acceptance checklists (for Section I shipments) and an external inspection of packages are the primary methods for operators to determine whether a package conforms to the regulations. However, acceptance checklists can only verify that the quantity is within limits, the packaging is undamaged, and the marks and labels accord with the dangerous goods transport document, and the external inspection of Section II shipments may be cursory. Damaged or improperly packaged lithium batteries and equipment are not readily identifiable through a physical inspection.

f) Design testing and quality control at the point of manufacture of cells and batteries are the primary proactive measures in the Technical Instructions aimed at controlling hazards of lithium batteries either packed with or contained in equipment.

g) A state of charge requirement is most practically implemented by the offeror or the original manufacturer. Verifying compliance with a state of charge requirement is impractical once packages are prepared and offered for transport.

2. DISCUSSION BY THE DGP-WG

2.1 The DGP is invited to review the report in the appendix and consider the findings.

— — — — — — — —

APPENDIX

A SYSTEM THEORETIC APPROACH TO THE SAFE CARRIAGE OF LITHIUM BATTERIES BY AIR

CONTENTS

EXECUTIVE SUMMARY

Purpose and method of this report

The DGP created the working group on energy storage devices to progress the work identified in ANC job card DGP.003.03 mitigating safety risks posed by the carriage of lithium batteries by air. During DGP/28, the panel requested the DGP-WG/Energy Storage Devices conduct of a safety risk assessment on lithium batteries packed with or contained in equipment and vehicles. The working group was tasked with conducting a safety risk assessment on extending the existing state of charge limit for UN 3480 to UN 3481, particularly for lithium ion batteries packed with equipment. The DGP-WG/Energy Storage Devices applied Systems Theoretic Process Analysis (STPA) to explore the hazards associated with the air transport of lithium ion batteries packed with and contained in equipment. Existing safety requirements and potential new requirements were assessed against a mitigation order of precedence scale. The nine-person cross functional team that completed the actual analysis was composed of experts from air operations, aircraft design and manufacturing, and dangerous goods. The facilitator was an expert from the ICAO safety management section and trained in the STPA methodology but had little familiarity with the transport of dangerous goods.

The aim of this report is to provide an alternate perspective analysis of the hazards associated with the transport of lithium batteries by aircraft. Traditional risk assessment methods involve some type of probabilistic risk assessment that applies statistical or other analytical techniques to support decision making. Risk in this context is characterized as a product of the probability of an event occurring and the consequence. The basic approach assumes that incidents are caused by a component failure. Calculating the probability of failure of each component separately, and later combining them results in a likelihood. Decision makers can then determine whether this figure is acceptable or if not acceptable take actions to reduce either the likelihood or the consequence. The outputs from these analyses when applied to lithium battery transport have been unconvincing because these methods rely upon certain information and assumptions that do not apply here. First, these techniques rely on detailed data on the system and its components including a discrete number of shipments and packages, specifics of the package contents such as whether packages contained equipment or equipment and spare batteries and the types of equipment, incident rates, the specific cause of the incident, and factors that contribute to incidents. Such information is largely unavailable or insufficiently detailed to inform a standard analysis. Lithium battery incidents are low-probability events with outsized consequences and thus the predictability of such events is suspect. Second, it assumes that observations of past behaviour allow accurate prediction of future behaviour. The fast pace of technological change, new system entrants and an evolving regulatory landscape create cases where previous knowledge of system is of little benefit in generating probabilities. The STPA method overcomes many of these limitations by emphasizing interactions between system components and identifying ways that interactions violate system constraints. Hazards in this case are the product of flawed interactions between system components including operational factors, social interaction, physical components etc. Further, since STPA aims to prevent losses, this type of analysis is not limited to previously identified failures.

Findings and conclusions

Battery manufacturers, shippers, and ground handling service providers were identified as those controllers whose actions most directly led to hazards and losses. Applying STPA derived causal scenarios against existing requirements helps identify gaps and opportunities for new strategies to mitigate hazards. The group also identified the following broad themes:

a) The supply chain for lithium batteries and devices is fragmented and has many interactions amongst supply chain participants that introduce the possibility of safety issues.

b) The dangerous goods air transport system is based on trust whereby downstream supply chain participants e.g. operators rely on information provided by entities further up the chain e.g. battery and equipment manufacturers, and shippers. However, these entities (battery or equipment manufacturer, shipper, freight forwarder, operator and the civil aviation authority) are often disconnected.

c) A shipment prepared for transport may pass through multiple intermediaries such as freight forwarders and logistics agents who may not actually see a consignment. As such compliance with requirements is often assured only through the provision of suitable documentation and inspections immediately prior to loading.

d) Checklists and an external inspection of packages are the primary methods for operators to determine whether a package conforms to the regulations. However, acceptance checklists can only verify that the quantity is within limits, the packaging is undamaged, and the marks and labels accord with the dangerous goods transport document, and the external inspection of Section II shipments may be cursory.

e) Civil aviation authorities obtain most of their information on safety performance through incident reports and inspections.

When considering additional requirements, they should be targeted at eliminating or reducing hazards posed by batteries and equipment thereby mitigating many of the problems associated with mishandling or damage which may occur during preparation for transport, and during transport. While the ICAO can add requirements to the Technical Instructions, national authorities are responsible for oversight. Manufacturers, shippers, and operators are responsible for complying with the provisions of the regulations. Collaborative work with all supply chain participants, will be necessary to ensure requirements are met.

1. INTRODUCTION

1.1 Overview and organization of the report

This report applies the systems theoretic process analysis (STPA) method to the air transport of lithium ion batteries packed with and contained in equipment. Section 2 explains the basic STPA method and introduces a means to rank the strength of potential mitigations. Sections 3, and 4 apply STPA to explore the safe carriage of lithium ion batteries and lithium ion battery powered equipment by air. Section 5 details analysis conclusions and potential future work. The attachment provides detailed tables that identify controller responsibilities, various unsafe control actions, causal scenarios and definitions of terms used in this report.

2. METHODOLOGY

2.1 STPA

The STPA method starts from a stakeholder prioritized list of system losses, followed by identifying high level hazards (system states) that can lead to those losses. Causal scenarios (including non-failures) that lead to hazards are considered. Identifying causal scenarios that do not involve failures but nevertheless result in hazardous conditions is an important feature of STPA and could encourage healthy scepticism of our knowledge of the system and promote decisions not only on what we know, but what we do not know. The basic STPA method involves (4) four steps.

Define the purpose of the analysis

- Identify losses (injury or loss of life, aircraft or cargo, mission)
- Identify system-level hazards (fire, damaged batteries in transport)
- Identify system-level constraints

Model the control structure

- System model consisting of control-feedback loops
- Control structure enforces constraints across the system

Identify unsafe control actions

- Control action that in a particular context and worst-case environment, will lead to a hazard
- Identify the behaviors that should be prevented

Identify causal scenarios

- Why would unsafe control actions occur?
- Why would control actions be improperly executed or not executed, leading to hazards?

Following completion of Step 4, mitigation measures can be identified and discussed in view of whether measure(s) prevent, reduce, or mitigate unsafe control actions (UCAs) or the occurrence of causal scenarios that lead to system hazards. In this case the strength of mitigation measures could be ranked based on a hierarchy where controls that prevent the occurrence of a UCA through system design are especially powerful, followed by controls that mitigate UCAs, followed by controls that increase detection of UCAs and controls involving additional procedures and training.

2.2 Mitigation effectiveness

The Technical Instructions identify the acceptability of lithium ion batteries and battery powered devices for transport by air and under what conditions. As such, the Technical Instructions include many requirements intended to prevent and mitigate these causal scenarios. As previously discussed, standard risk assessment methods and risk matrix are not well suited to examining lithium battery transport safety. Leveson, 2019 suggests using STPA and replacing hazards for failures and redefining likelihood based on the strength of potential controls. The relationship between individual failures and incidents is rarely obvious and it is nearly impossible to reliably assess the likelihood of future incidents based on previous experience. To overcome these obstacles the group utilized a mitigation order or precedence scale consistent with MIL-STD-882 and various other safety standards. Mitigations that design for minimum risk or eliminate the risk are ranked higher than those mitigations that provide only warnings or rely on procedures and training.

Table 1. Mitigation level order of precedence

Mitigation level	Mitigation description	Mitigation effectiveness score
Design for minimum risk	The causal factor can be eliminated through design to eliminate risks.	5
Reduction through design	If the identified risks cannot be eliminated, reduce it to an acceptable level through design selection e.g., safety design features or safety devices. The occurrence of the casual factor can then be reduced or controlled through system design (proactive)	4
Provide warning devices	When neither design nor safety devices can eliminate identified risks or reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal. The causal factor can be detected and requires a response to mitigate (reactive).	3
Develop training and procedures	Where it is impractical to eliminate risks through system design, training and procedures are used. Causal factor can be mitigated through additional training and procedures (reactive)	2
None	No possible mitigation exists, or mitigation is never applied	1

Existing mitigations found in the Technical Instructions were identified and assigned a mitigation effectiveness score based on this ranking. Suggested mitigations to the scenarios generated by the STPA and mitigation effectiveness scores are presented later in this report.

Table 2. Existing mitigations

Description	Mitigation effectiveness score
UN 38.3 testing and quality management system	4
UN 38.3 test summary	3
Strong rigid outer packaging. Acceptable package types and performance qualities identified	4
Requirements to protect equipment against short circuits and damage	4
Package/overpack marks, labels, and documentation indicate the presence of lithium batteries in a consignment	3

Description	Mitigation effectiveness score
Initial acceptance check	2
Inspection prior to loading	2
Handling procedures and personnel training	2

3. APPLYING STPA TO SUPPORT THE SAFE CARRIAGE OF LITHIUM BATTERIES BY AIR

3.1 Goals, requirements, and constraints

This analysis supports the evaluation of the continued safe and efficient air transport of lithium batteries packed with and contained in equipment. Consistent with the STPA technique, the ESD working group identified system level losses to prevent. Losses are defined here as anything of value to any stakeholder in the system.

Table 3. System level losses

Loss ID	Loss description
L1	Loss of aircraft
L2	Loss of human life or injury
L3	Loss of cargo
L4	Loss of confidence in the air transport system
L5	Loss of means to effectively transport lithium batteries (mission)

3.2 System-level hazards

Once system level losses are defined, system level hazards can be identified. Hazards are developed by linking losses to a set of conditions that combined with a worst-case environmental condition could lead to a loss. This does not necessarily guarantee that a hazard will always result in a loss. System level hazards here are restricted to those which can be controlled or managed by controllers within the system. The goal of the analysis is to eliminate or mitigate hazards that can lead to losses.

Table 4. System-level hazards

System hazard ID	Hazard description	Loss link
H1	Aircraft cargo compartment containing lithium batteries experiences a fire	L1-L5
H2a	Aircraft cargo compartment contains damaged lithium batteries	L3
H2b	Aircraft cargo compartment contains defective lithium batteries	L3
H2c	Aircraft cargo compartment contains untested lithium batteries	L4, L5

System hazard ID	Hazard description	Loss link
H3	Aircraft cargo compartment contains non-compliant lithium battery consignments	L4, L5

3.3 System-level safety constraints

System level safety constraints identify those conditions or behaviours that must be satisfied to eliminate hazards or minimize losses should a hazard occur. Each safety constraint is linked to a specific loss identified in [square brackets].

Table 5. System level constraints

System constraint ID	System constraint description
SC1	Fire in aircraft cargo compartment must be prevented [H1]
SC2	If fire in aircraft cargo compartment occurs, it must be detected, and appropriate measures taken to prevent loss [H1]
SC3	Damaged lithium batteries must not be transported by air [H2a]
SC4	If lithium batteries are damaged, they must be detected, and appropriate measures taken to prevent transport by air [H2a]
SC5	Defective lithium batteries must not be transported by air [H2b]
SC6	If lithium batteries are defective, they must be detected, and appropriate measures taken to prevent transport by air [H2b]
SC7	If lithium batteries are untested, they must be identified and approved for transport [H2c]
SC8	Shippers must only offer lithium batteries that comply with relevant requirements [H3]
SC9	If lithium batteries are not compliant with relevant requirements, they must be detected, and appropriate measures taken to prevent transport by air [H3]

3.4 Control structures

The group constructed a high-level hierarchical control structure and several detailed control structures of the lithium battery air transport system. The high-level control structure helps identify the various entities responsible for the safe carriage of lithium batteries in air transport. High level controllers include international organizations and national authorities responsible for the development and implementation of basic safety requirements. Lower-level controllers include shippers/packers and battery manufacturers responsible for preparing shipments and testing batteries and equipment. The high-level control structure and each detailed control structure is composed of feedback control loops. Each control structure contains the following elements:

a) Controllers;

b) Control actions;

c) Feedback;

d) Other inputs to and outputs from components (neither control nor feedback); and

e) Controlled processes.

In this hierarchical control structure vertical placement is meaningful. The vertical placement of a control structure entity represents control from high-level controllers at the top to the lowest-level entities (controlled processes) at the bottom. Each entity has control and authority over the entities immediately below it, and each entity is likewise subject to control and authority from the entities immediately above. Control and feedback processes are denoted by downward and upward arrows. Coordination between entities is denoted by two-way arrows and inputs are depicted as one-way horizontal arrows. Note that control does not guarantee obedience. The control and feedback flows in the control structure identified as downward and upward arrows respectively simply indicate that a control or feedback mechanism exists. Just because a controller sends a command, does not mean in practice that it is received or if received that it will be followed. Similarly, just because a feedback path is included in the control structure, does not mean that the feedback will always be sent and if sent that the feedback is accurate. The diagram below is a basic control structure that identifies the major entities responsible for developing and enforcing safety requirements for a consignment of lithium batteries and equipment. A more detailed control structure that includes additional entities including freight forwarders, standards development organizations, and other international entities is included in the attachment to this report.

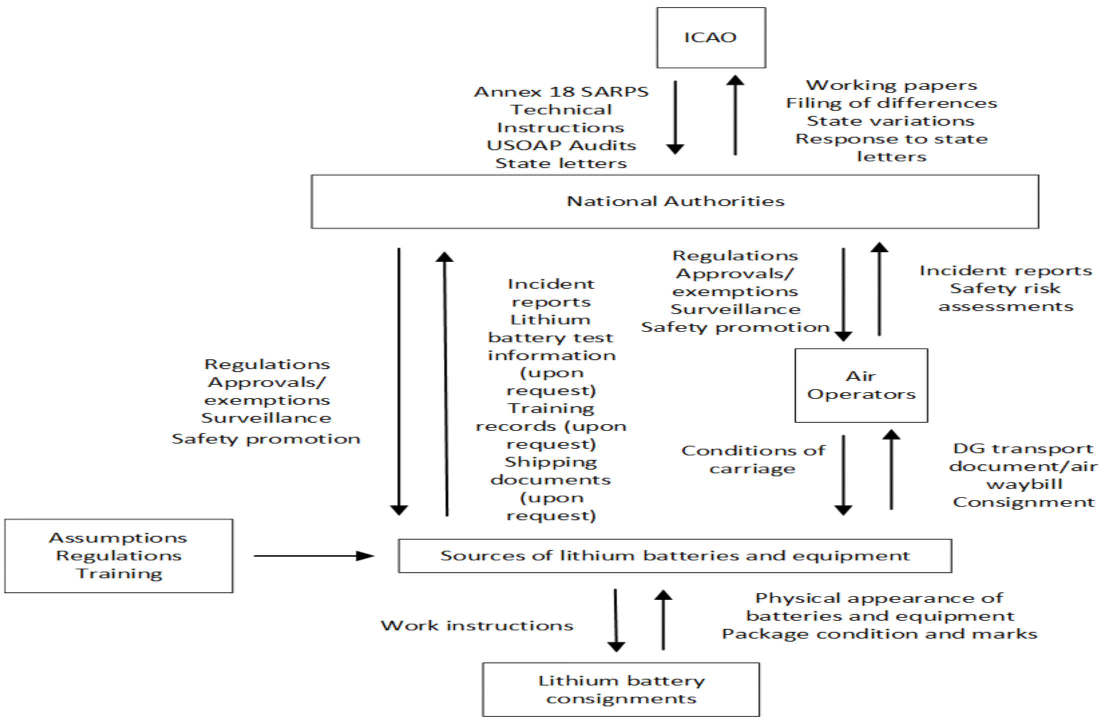


Figure 1. High level control structure

Detailed control structures

The group developed detailed control structures of various components of the high-level control structure that identify the relationships between various entities. Completing several detailed control structures around different parts of the control structure allows for a more complete analysis of the safety control actions designed to help the system enforce constraints and the feedback received. The figures below show detailed control-feedback loops for various controllers. These figures include inputs, decision making processes such as procedures or work instructions and beliefs/mental models of each of these controllers. These additions help identify and develop unsafe control actions and causal scenarios.

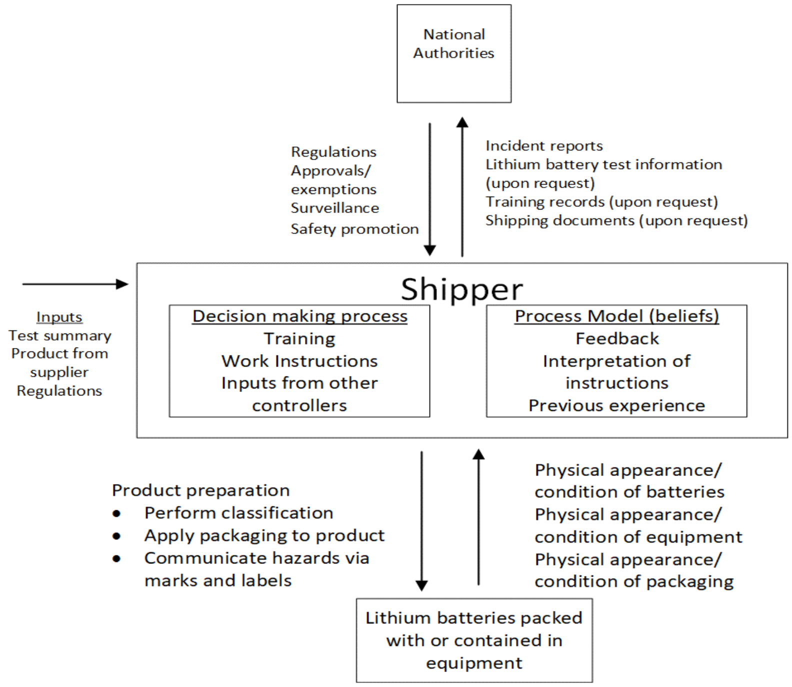


Figure 2. Control-feedback loop for a shipper

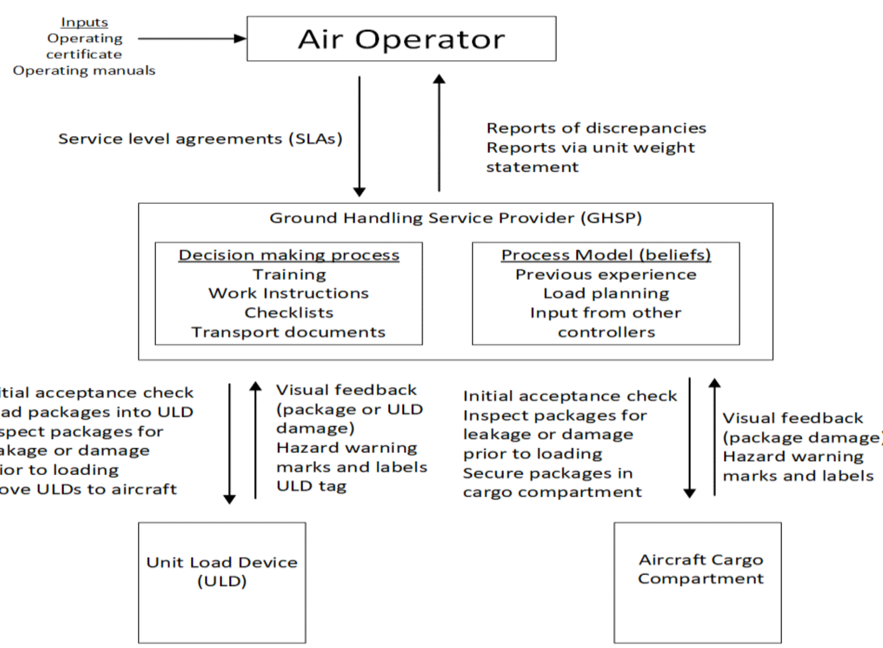


Figure 3. Control feedback loop for a ground handling service provider

`

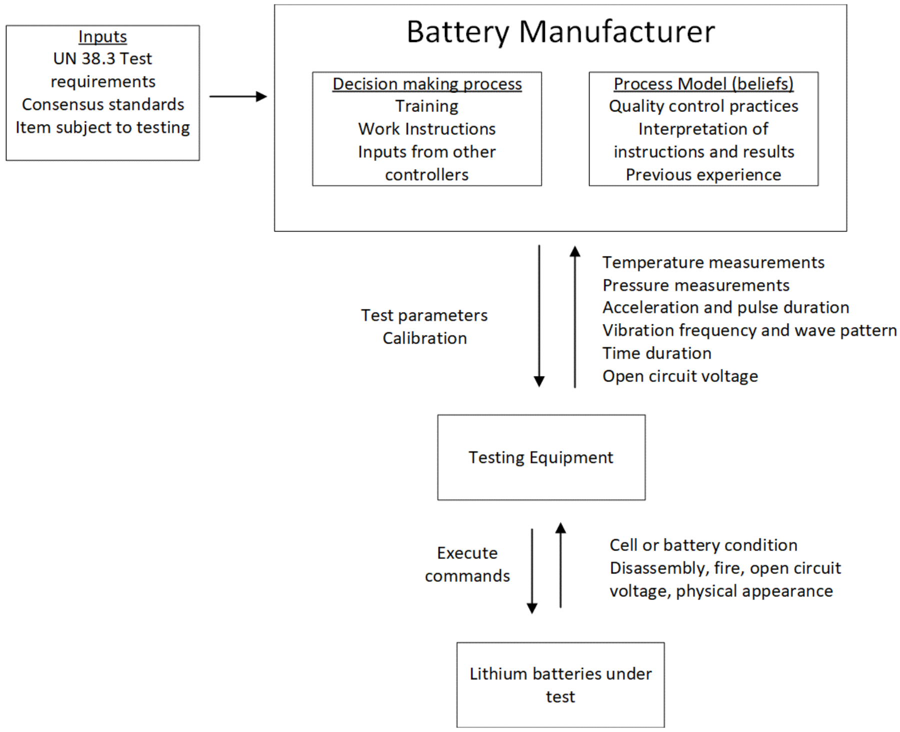


Figure 4. Control-feedback loop for a battery manufacturer

3.5 Identifying unsafe control actions

Each controller in the system has certain responsibilities depicted as downward facing arrows. These responsibilities enforce safety constraints to prevent system level hazards. In this context, an unsafe control action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a system level hazard. STPA identifies four (4) ways that a control action may violate safety constraints:

a) Providing the control action leads to a hazard.

b) Not providing the control action leads to a hazard.

c) Providing a potentially safe control action but too early, too late, or in the wrong order.

d) The control action lasts too long or is stopped too soon (for continuous control actions, not discrete actions).

For example, a shipper does not apply appropriate marks, labels, or indicate the presence of lithium batteries in a consignment before offering for transport. [H3]

This action is unsafe because it can lead to H3: Aircraft cargo compartment contains non-compliant lithium battery consignments.

In another example, a shipper prepares a consignment of lithium batteries packed with equipment for transport without consulting applicable regulations [H1, H2, H3].

This action is unsafe because it could lead to [H1 - Aircraft cargo compartment containing lithium batteries experiences a fire], [H2a - Aircraft cargo compartment contains damaged lithium batteries], and [H3 - Aircraft cargo compartment contains non-compliant lithium batteries]. While the shipper utilizes packaging, since the shipper does not consult the applicable requirements, the packaging may not be sufficient for transport, or the contents not properly prepared and may become damaged. In a particular set of worst-case conditions, this damage could lead to a fire in the aircraft cargo compartment. Section 5.4 contains tables that identify unsafe control actions for various controllers including shippers, ground handling service providers, and battery manufacturers.

3.6 Identifying causal scenarios associated with unsafe control actions

Once unsafe control actions were compiled, the group identified the causal factors that lead to the unsafe control actions, which in turn led to hazards and by extension, to losses. Working backwards from the UCAs, this produces a list of contextualized scenarios that help explain why an unsafe control action occurred. Generally, causal scenarios explain how incorrect or inadequate feedback, information exchange, and other factors contribute to losses. The scenarios also explain how control actions when provided might not be received or improperly executed. Section 5.5 contains a table listing the various causal scenarios connected to unsafe control actions.

In the previous example of a shipper who does not apply appropriate marks, labels, or indicate the presence of lithium batteries in a consignment before offering for transport [H3] a causal scenario leading to this unsafe action follows.

Scenario: The shipper does apply not apply appropriate marks, labels or indicate the presence of lithium batteries in or with equipment prior to offering a package for transport [H3]. The shipper typically does not offer dangerous goods for transport and did not recognize that lithium batteries and battery powered equipment are regulated as dangerous goods. As a result, since there are no identifying marks, these non-compliant packages are undetected by the operator and loaded onto the aircraft.

4. RISK EVALUATION

4.1 Identifying mitigations to causal scenarios

The energy storage device working group identified UCAs and causal scenarios involving various controllers in the air transport system. The group identified battery manufacturers, shippers, and ground handling service providers as those controllers whose actions most directly led to hazards and losses. Following an analysis of the system using STPA, the working group developed a list of recommended mitigations or new requirements and applied a mitigation effectiveness score.

Table 6. Potential additional requirements scored against the mitigation order of precedence

Causal scenario ID	Causal scenario description	Recommended mitigation description	Mitigation effectiveness score
CS 1.1	Manufacturers do not complete UN38.3 tests.	National authorities conduct inspections and surveillance on battery/equipment manufacturers to identify flawed assumptions in the battery testing and equipment environment and conditions that violate assumptions about usage conditions.	3
		Develop detailed requirements to identify acceptable design changes.	2
		Reduce the state of charge for rechargeable batteries.	4
CS 1.2	Manufacturers do not develop and adhere to a quality management system.	Develop detailed requirements for quality assessments including third-party verification.	2
		Develop safety features for battery powered equipment	4
		Reduce the state of charge for rechargeable batteries.	4
CS 1.3	Shipper does not utilize lithium battery test summary information to make a classification decision.	Require shippers to produce lithium battery test summaries as a condition for carriage	2
CS 2.1	Shipper does not protect the battery from short circuits or damage prior to placement of the battery in the package with equipment.	Increase awareness of shipping and transport requirements	2
		Require training for all shippers	2
		Reduce the State of charge for rechargeable batteries	4
		Design equipment to protect installed batteries	4
CS 2.2	Shipper/packer does not secure equipment within the outer packaging when offering for transport	Increase awareness of shipping and transport requirements	2
		Require training for all shippers	2
		Reduce the State of charge for rechargeable batteries	4

Causal scenario ID	**Causal scenario description**	**Recommended mitigation description**	**Mitigation effectiveness score**
		Design equipment to protect installed batteries	4
CS 3.1	Shipper/ packer selects a package of insufficient strength leading to damage of the contents during handling.	Increase awareness of shipping and transport requirements	2
		Require training for all shippers	2
		Reduce the state of charge for rechargeable batteries	4
		Design equipment to protect installed batteries	4
CS 3.2	Ground handling service provider damages packages during handling	Require quarantine or inspection of all packages subject to suspected damage	3
		Reduce the state of charge for rechargeable batteries	4
		Design equipment to protect installed batteries	4
		Review training and procedures for package handlers	2
CS 4.1	Shipper does not apply appropriate marks, labels, or indicate the presence of lithium batteries in a consignment.	Eliminate provisions that allow consignments to be transported without identifying marks and documentation	3
		Require training for all shippers	2
		Reduce the state of charge for rechargeable batteries	4
		Design equipment to protect installed batteries	4
4.2	Operator accepts a consolidation of multiple consignments of lithium batteries contained in equipment in a mail sack without marks, labels, and declaration.	Eliminate provisions that allow consignments to be transported without identifying marks and documentation	3
		Require training for all mailers	2
		Reduce the state of charge for rechargeable batteries	4
		Institute requirements for mailers to indicate the presence of electronic equipment or items containing batteries or attest to the absence of electronic equipment containing lithium batteries.	2

5 CONCLUSION

The Technical Instructions identify the conditions in which lithium ion batteries and battery powered devices can be accepted for transport by air. These conditions identified as requirements and packing instructions are intended to ensure that the safety of dangerous goods in air transport is assured. Effectiveness of requirements can be inferred by a reduction of incidents from a specific cause, but little can be said about overall system safety other than incidents continue to occur. Compliance with safety requirements is verified using checklists, comparing a consignment with the package and documents provided by shippers, and a physical inspection. However, damaged, or improperly packaged lithium batteries and equipment are not readily identifiable through a physical inspection. Shipments that do not have visible marks or labels or shipping documents that identify the consignment as dangerous goods, are not subject to additional checks required for dangerous goods. The DGP-WG/Energy Storage Devices identified several themes throughout its analysis.

a) The supply chain for lithium ion batteries and devices is fragmented and has many interactions amongst supply chain participants that introduce the possibility of safety issues.

b) The dangerous goods air transport system is based on trust whereby downstream supply chain participants e.g. operators rely on information provided by entities further up the chain e.g. battery and equipment manufacturers, and shippers. However, these entities (battery or equipment manufacturer, shipper, freight forwarder, operator and the civil aviation authority) are often disconnected.

c) A shipment prepared for transport may pass through multiple intermediaries such as freight forwarders and logistics agents who may not actually see a consignment. As such compliance with requirements is often assured only through the provision of suitable documentation and inspections immediately prior to loading.

d) Checklists (for Section I shipments) and an external inspection of packages are the primary methods for operators to determine whether a package conforms to the regulations. However, acceptance checklists can only verify that the quantity is within limits, the packaging is undamaged, and the marks and labels accord with the dangerous goods transport document, and the external inspection of Section II shipments may be cursory.

e) Civil aviation authorities obtain most of their information on safety performance through incident reports and inspections..

f) While the ICAO can add requirements to the Technical Instructions national authorities are responsible for oversight. Manufacturers, shippers, and operators are responsible for complying with the provisions of the regulations. Collaborative work with all supply chain participants, will be necessary to ensure requirements are met.

g) Additional requirements should be targeted at maximizing safety throughout the supply chain and work with supply chain participants to develop a means to ensure requirements are met.

5.1 Future work

The working group on energy storage devices developed detailed control structures and unsafe control actions for battery manufacturers, shippers, and ground handling service providers. Additional work could focus on the exploring the relationships between the original shipper, intermediaries including freight forwarders, indirect air carriers and the operator. These entities do not move cargo but instead contract with an operator and may assume the role of the shipper. The relationship between mailers, designated postal operators, national competent authorities and operators is another aspect of the control structure identified but not investigated in this report. The control structure depicting battery testing could be revisited to further identify specific inputs and feedback to derive detailed UCAs and causal scenarios that lead to the presence of low-quality batteries. Processes that involve battery assembly and integration of batteries into equipment and equipment testing could also be explored to identify how batteries that otherwise comply with testing can create safety hazards.

ATTACHMENT

GLOSSARY OF TERMS

This report utilizes various terms used in normal parlance that denote a specific meaning within the context of this report. The following table defines many of these terms, derived or adapted from the STPA handbook.

Causal factor	A causal factor is an element that contributes to unsafe control actions and eventually system-level hazards.
Causal scenario	A causal scenario describes the contributing factors that cause unsafe control actions, why they could happen and how these causal factors lead to system-level hazards.
Control algorithm	The control algorithm represents the controller’s decision-making process—it determines the control actions to provide.
Control action	A control action is the bringing about of an alteration in the system's state through activation of a device or implementation of a procedure with the intent of regulating or guiding the operation of a human being, machine, apparatus, or system.
Controller	The controller provides control actions on the system and gets feedback to determine the impact of the control actions. The controller enforces constraints on the behaviour of the system.
Feedback	Feedback includes evaluative or corrective information about an action, event, or process that is transmitted to the original or controlling source.
Loss	A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.
Process model	Process models represent the controller’s internal beliefs used to make decisions. Process models may include beliefs about the process being controlled or other relevant aspects of the system or the environment.
System-level constraint	A constraint specifies system conditions or behaviours that need to be satisfied to prevent hazards (and ultimately prevent losses).
System-level hazard	A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.
Unsafe control action	An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard.

SYSTEM-LEVEL LOSS TABLE

The below table shows system level losses identified by the DGP-WG/Energy Storage Devices.

Loss ID	Loss description
L1	Loss of aircraft
L2	Loss of human life or injury
L3	Loss of cargo
L4	Loss of confidence in the air transport system
L5	Loss of means to effectively transport lithium batteries (mission)

SYSTEM-LEVEL HAZARD TABLE

The below table shows system level hazards identified by the DGP-WG/Energy Storage Devices. System-level hazards are linked to specific losses.

System hazard ID	Hazard description	Loss link
H1	Aircraft cargo compartment containing lithium batteries experiences a fire	L1-L5
H2a	Aircraft cargo compartment contains damaged lithium batteries	L3
H2b	Aircraft cargo compartment contains defective lithium batteries	L3
H2c	Aircraft cargo compartment contains untested lithium batteries	L4, L5
H3	Aircraft cargo compartment contains non-compliant lithium battery consignments	L4, L5

SYSTEM RESPONSIBILITIES

The responsibilities involve providing control actions and receiving feedback, thus creating the control-feedback loops of the **high-level control structure**.

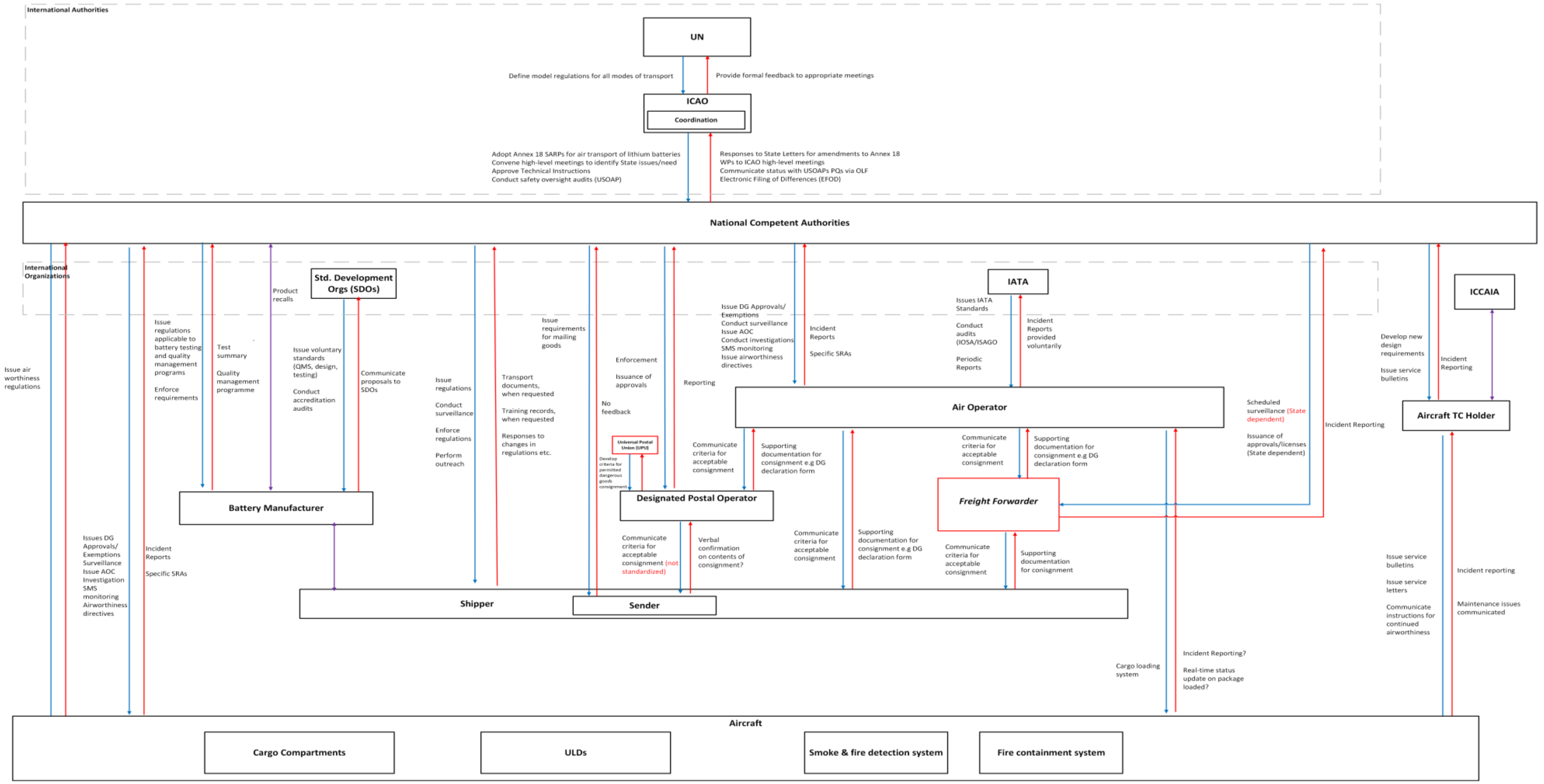
The controller and their responsibilities are identified in the context of the mission (i.e., continued safe and efficient air transport of lithium batteries packed with and contained in equipment).

System responsibilities	
Controller	**Description**
International Civil Aviation Organization (ICAO)	— Defines international Standards and Recommended Practices (SARPs), the Technical Instructions, and guidance material aimed at industry for the safe transport of dangerous goods by air — Establishes responsibilities for States — Conducts audits through its Universal Safety Oversight Audit Program (USOPA) on States for compliance with ICAO SARPs (Annex 6, Annex 18)
National competent authorities (NCA)	— Promulgate regulations for the safe transport of dangerous goods by air — Promulgate regulations for required aircraft features e.g handheld fire extinguishers, fire suppression systems — Conduct inspections and surveillance of air operators and other entities that offer dangerous goods for transport by air — Enforce regulations on regulated entities (e.g air operators, shipper, freight forwarders, designated postal operators (DPOs), ground handling service providers (GHSPs), packaging manufacturer) where non-compliance with Technical Instructions is identified — Issue air operator certificates (AOCs) — Issue specific approval for operator to carry dangerous goods as cargo — Approve policies, procedures and training developed by DPO — Grant approvals or exemptions for the transport of dangerous goods incl. lithium batteries — Investigate occurrences — Ensure operator conducts safety risk assessments of cargo compartment safety
Battery manufacturer or distributor	— Produces and distributes batteries that have passed all applicable UN 38.3 tests — Implements a quality management programme for the manufacture of lithium cells and batteries — Makes available UN 38.3 test summary

System responsibilities	
Controller	**Description**
Shipper/consignor/packer	— Ensure that employees tasked with preparing shipments are competent to perform the tasks — Classify lithium batteries and products with lithium content based in accordance with the Technical Instructions — Pack, mark, and label packages in accordance with the Technical Instructions prior to shipment — Complete dangerous goods transport document describing dangerous goods offered for transport in accordance with Part 5;4 of the Technical Instructions or provide appropriate information to be included on the air waybill, as applicable
Airline operations	— Document policies and procedures for the acceptance and handling of dangerous goods — Ensure that employees tasked with accepting and handling dangerous goods are competent to perform the task — Develop and implement effective controls to prevent the introduction of dangerous goods not in accordance with the Technical Instructions Chapter 7;6.1 — Conduct acceptance checks when triggered (with specific exceptions with respect to lithium batteries) — Perform safety risk assessment on cargo compartment safety — Review safety risk assessment based on change to operation and incidents that indicate risk mitigations may not be adequate (Doc 10102, guidance) — Report dangerous goods incidents to the NCA in accordance with the Technical Instructions — Develop and implement a process for investigation of reported incidents and identification and verification of appropriate corrective actions
Cargo compartment	Contain packages (different classes exist that meet certain regulatory standards concerning accessibility, a means to exclude hazardous quantities of smoke or extinguishing agent, smoke a fire detection, and a means to extinguish or control a fire)
Ground handling service provider (operator and/or 3rd party)	— Documents policies and procedures for the handling of dangerous goods — Ensures that employees tasked with handling dangerous goods are competent to perform the task — Loads/unloads packages into cargo compartment — Secures packages in cargo compartment — Secures packages in unit load device
Unit load devices (ULDs)	Contain packages in a single consolidation to provide protection or convenience of handling. Examples include any type of freight container, aircraft container, or aircraft pallet with a net. Some ULDs also have fire-resistant capabilities — no regulatory requirement for fire resistance.

CONTROL STRUCTURE

A high-level hierarchical control structure of the lithium battery air transport system was developed to identify and analyse the various entities responsible for the safe carriage of lithium batteries in air transport. High level controllers include international organizations and national authorities responsible for the development and implementation of basic safety requirements. Lower-level controllers include shippers/packers and battery manufacturers responsible for preparing shipments and testing batteries and equipment. This control structure includes additional entities not covered in this analysis including freight forwarders, standards development organizations and other international organizations.


International Authorities
UN
Define model regulations for all modes of transport
Provide formal feedback to appropriate meetings
ICAO
Coordination
Adopt Annex 18 SARPs for air transport of lithium batteries
Convene high-level meetings to identify State issues/need
Approve Technical Instructions
Conduct safety oversight audits (USOAP)
Responses to State Letters for amendments to Annex 18
WPs to ICAO high-level meetings
Communicate status with USOAPs PQs via OLF
Electronic Filing of Differences (EFOD)
National Competent Authorities
International Organizations
Std. Development Orgs (SDOs)
IATA
ICCAIA
Issue air worthiness regulations
Issue regulations applicable to battery testing and quality management programs
Enforce requirements
Test summary
Quality management programme
Product recalls
Issue voluntary standards (QMS, design, testing)
Conduct accreditation audits
Communicate proposals to SDOs
Issue regulations
Conduct surveillance
Enforce regulations
Perform outreach
Issue requirements for mailing goods
Transport documents, when requested
Training records, when requested
Responses to changes in regulations etc.
Enforcement
Issuance of approvals
No feedback
Reporting
Issue DG Approvals/ Exemptions
Conduct surveillance
Issue AOC
Conduct investigations
SMS monitoring
Issue airworthiness directives
Incident Reports
Specific SRAs
Issues IATA Standards
Conduct audits (IOSA/ISAGO
Periodic Reports
Incident Reports provided voluntarily
Develop new design requirements
Issue service bulletins
Incident Reporting
Air Operator
Aircraft TC Holder
Scheduled surveillance (State dependent)
Issuance of approvals/licenses (State dependent)
Incident Reporting
Universal Postal Union (UPU)
Develop criteria for permitted dangerous goods consignment
Communicate criteria for acceptable consignment
Supporting documentation for consignment e.g DG declaration form
Communicate criteria for acceptable consignment
Supporting documentation for consignment e.g DG declaration form
Battery Manufacturer
Designated Postal Operator
Freight Forwarder
Issues DG Approvals/ Exemptions
Surveillance
Issue AOC
Investigation
SMS monitoring
Airworthiness directives
Incident Reports
Specific SRAs
Communicate criteria for acceptable consignment (not standardized)
Verbal confirmation on contents of consignment?
Communicate criteria for acceptable consignment
Supporting documentation for consignment e.g DG declaration form
Communicate criteria for acceptable consignment
Supporting documentation for conisgnment
Issue service bulletins
Issue service letters
Communicate instructions for continued airworthiness
Incident reporting
Maintenance issues communicated
Shipper
Sender
Cargo loading system
Incident Reporting?
Real-time status update on package loaded?
Aircraft
Cargo Compartments
ULDs
Smoke & fire detection system
Fire containment system

UNSAFE CONTROL ACTIONS

The STPA specifies four ways a control action can be unsafe (represented in the columns below). Highlighted unsafe control actions are also reflected in causal scenarios:

Control Action	Control action provided	Control action not provided	Control action provided too early/too late	Control action stopped too soon or applied too long
Cell/Battery Manufacturer Complete UN 38.3 Tests Subject lithium batteries to UN 38.3 design tests Part 2;9	Battery manufacturer completes UN 38.3 tests on battery with the wrong input information [H2c, H3]	Battery manufacturer does not subject lithium batteries to UN 38.3 tests [H2c, H3]	Battery manufacturer completes UN 38.3 tests before subsequent changes are made to battery design [H2c, H3]	Battery manufacturer completes UN 38.3 tests in incorrect sequence [H2c, H3]
Cell/Battery Manufacturer Provide Lithium Battery Test Summary Develop and make available a lithium battery test summary	Battery manufacturer provides test summary for a battery different than that tested [H2c, H3]	Battery manufacturer does not make available test summary information [H2c, H3]	Battery manufacturer provides test summary information after subsequent shipper has offered the battery for transport [H3]	Battery manufacturer provides out of date test summary information [H3]
Cell/Battery Manufacturer Manufacture under a quality management programme	N/A	Battery manufacturer does not develop and adhere to a quality management system while producing batteries [H2b, H3]	Battery manufacturer quality management programme applied after design defects are discovered [H2b, H3]	Battery manufacturer continues to apply the same quality management programme without updating to account for changes in design or inputs [H2b, H3]

Control Action	Control action provided	Control action not provided	Control action provided too early/too late	Control action stopped too soon or applied too long
Shipper Classify product The shipper must ensure the goods are not forbidden for transport by aircraft and ensure the goods are properly classified as required by the Technical instructions.	N/A	Shipper does not classify product prior to offering for transport [H3]	Shipper classifies product after offering for transport [H3]	N/A
Shipper Apply packaging Adhere to inner packaging and the maximum quantity per package limits. Select appropriate types of packaging according to the packing instructions. Apply closures to inner and outer packagings as appropriate. Secure packages within an overpack when applicable.	Shipper applies packaging without consulting applicable requirements when offering for transport [H1, H2a, H2c, H3]	Shipper does not pack product in strong rigid outer packaging when offering for transport [H1, H2a, H3] Shipper does not secure equipment within the outer packaging when offering for transport [H1, H2a, H3] Shipper does not protect the battery from short circuits prior to placement of the battery in the package [H1, H2a, H3]	N/A	N/A

Control Action	Control action provided	Control action not provided	Control action provided too early/too late	Control action stopped too soon or applied too long
Shipper Communicate hazards via marks, labels, and documents Apply appropriate marks and labels as required by the Technical Instructions. Complete transport documents and sign declaration when applicable	Shipper applies marks and labels to communicate hazards however visibility by is obscured [H3]	Shipper applies marks and labels that do not reflect the contents of the package [H3] Shipper does not apply appropriate marks, labels, or indicate the presence of lithium batteries in a consignment before offering for transport [H3]	N/A	Shipper applies marks and labels without completing documentation when offering for transport [H3] Shipper completes documentation however does not apply marks and labels when offering for transport [H3]

Control Action	Control action provided	Control action not provided	Control action provided too early/too late	Control action stopped too soon or applied too long
Ground Handling Service Provider/Operator Perform acceptance check	— Ground handling service provider performs acceptance check using checklist without inspecting the package for damage [H2a, H3] — Ground handling service provider performs acceptance check without the means to verify the information on form [H3] — Ground handling service provider performs acceptance check when it is not possible to validate all the information on checklist [H3]	Ground handling service provider does not perform acceptance check [H2a, H3]	Ground handling service provider performs acceptance check after packages are loaded into ULD [H2a, H3]	Ground handling service provider performs acceptance check on some but not all incoming packages prior to loading into ULD [H2a, H3]
Ground Handling Service Provider/Operator Inspect package for leakage/damage	N/A	Ground handling service provider does not inspect the package for leakage or damage prior to loading into ULD or aircraft cargo compartment [H1, H2a, H3]	N/A	Ground handling service provider does not perform any further inspections on package once it has been subjected to initial acceptance check [H1, H2a, H3]

Control Action	Control action provided	Control action not provided	Control action provided too early/too late	Control action stopped too soon or applied too long
Ground Handling Service Provider/Operator Loads packages into unit load device or aircraft cargo compartment Loads unit load device into aircraft cargo compartment	Ground handling service provider loads damaged packages into ULD or aircraft cargo compartment [H1, H2a] Ground handling service provider places excessive superimposed weight on packages [H1, H2a] Ground handling service provider places too many packages placed into a ULD [H1, H2a]	Ground handling service provider does not secure packages against excessive movement inside of ULD [H1, H2a] Ground handling service provider does not secure packages against excessive movement inside of aircraft cargo compartment [H1, H2a]	N/A	N/A

CAUSAL SCENARIOS TABLE

Causal scenarios are presented in the following tables as small stories that explain not only the contributing factors that cause unsafe control actions, why they could happen and resulting hazards.

CS ID	Unsafe control action	Causal scenario
1.1	Manufacturer does not subject lithium batteries to UN 38.3 testing and does not have a quality management system in place prior to offering for transport. [H2c, H3]	A manufacturer does not subject lithium batteries to UN 38.3 testing because they believed the product being manufactured was sufficiently similar to a tested design. Manufacturer creates a battery that is intended to mimic a brand name to a tested type (counterfeit) Battery assembler manufacturers batteries from tested cells but does not test the assembled battery
1.2	Manufacturer did not develop and adhere to a quality management system for battery manufacturing process while producing batteries. [H2b-H3]	QA process does not include ongoing surveillance and defects were not detected prior to distribution QA process not sufficient or non-existent introducing defects into battery products

CS ID	Unsafe control action	Causal scenario
1.3	Shipper does not utilize lithium battery test summary information to make a classification before offering a package containing lithium batteries for transport because… leading to potentially non-compliant batteries loaded into an aircraft cargo compartment. [H3]	The shipper did not obtain the test summary information. The manufacturer or distributor does not make available a lithium battery test summary. Battery in the device is of an unknown origin. The shipper believes this information is unnecessary to make classification decisions. The shipper has sufficient information for shipping purposes based on a physical examination. The test summary does not match the product in the package. The shipper has a refurbished device containing a battery that is different than the original battery reflected in the available test summary. The devices contain batteries from a product different from that originally manufactured and used.
2.1	Shipper/packer does not protect the battery from short circuits prior to placement of the battery in the package with equipment because… As a result, terminals contact electrically conductive material in the same package generating excessive heat leading to a fire. [H1, H2a, H3]	The shipper assumes that the terminals are inherently protected. The shipper utilizes a package that is too large for the contents and subsequent shifting of the contents damages the battery. Shipper/packer misunderstands, mis-interprets or is unaware of this requirement. Shipper/packer does not recognize the importance of short circuit protection. Shipper/packer assumes that battery is sufficiently protected from short circuits without additional action. Electrically conductive products are placed into the same package as a battery.

CS ID	Unsafe control action	Causal scenario
2.2	Shipper/packer does not secure equipment within the outer packaging when offering for transport because… As a result, equipment is damaged due to shifting of the equipment or other contents in the in the same package, overpack, or adjacent consignments. [H1, H2a, H3]	The shipper/packer assumes that the package is sufficient to protect the equipment without additional securement Shipper/packer misunderstands, mis-interprets or is unaware of this requirement or the presence of a lithium battery contained in the equipment Shipper/packer does not recognize the importance of protecting against damage Shipper/packer determines the equipment is sufficiently protected from damage without additional action Shipper/packer determines the equipment does not require an outer packaging
3.1	Shipper/packer selects a package of insufficient strength leading to damage of the contents during handling and damage not detected prior to loading into the aircraft cargo compartment leading. [H1, H2a, H3] As a result, package contents are damaged through stacking or other handling conditions typically encountered in transportation immediately prior to or after loading into the aircraft cargo compartment.	Shipper does not recognize the hazard associated with the product if damaged. Shipper does not use sufficient cushioning material to protect batteries from damage from other items in the same package. Shipper places an item in the package heavier than package capability. Shipper does not understand the packing requirements of the Technical Instructions and selects a package of insufficient durability.

CS ID	Unsafe control action	Causal scenario
3.2	Ground handling service provider damages packages during handling leading to damage to contents prior to loading into the aircraft cargo compartment leading. [H1, H2a] As a result, package contents are damaged due to abuse conditions immediately prior to or after loading into the aircraft cargo compartment.	Packages crushed from overtightening of nets or pallet straps Too many packages pushed through a mechanized sort system /chute at once Forklift tines or handling vehicles crush packages containing batteries and equipment Penetration of packaged from external source such as forklift tines Package is dropped from a height greater than that capable of withstanding Packages consolidated improperly leading to excessive superimposed weight Packages inspected prior to consolidation but damaged during subsequent handling
4.1	The shipper does not apply appropriate marks, labels, or indicate the presence of lithium batteries in a consignment before offering for transport because… As a result, the shipper offered non-compliant batteries for transport leading to the possibility that misclassified batteries/equipment are loaded into an aircraft cargo compartment. [H3]	The shipper did not recognize that lithium batteries and equipment are regulated as dangerous goods. For lithium batteries contained in equipment (including button cells on circuit boards) (2 batteries/4 cells) up to 2 packages per consignment shippers need not apply marks, labels or identify to the operator. Regulations create an incentive to classify batteries as equipment or batteries packed with equipment. Changes in the physical appearance of batteries e.g.., powerbanks leads to a shipper misclassify a battery as equipment. Shipper misclassifies certain a packaged batteries or a powerbank packed with an item of equipment as batteries packed with equipment.

CS ID	Unsafe control action	Causal scenario
4.2	Operator accepts a consolidation of multiple consignments of lithium batteries contained in equipment in a mail sack without marks, labels, and declaration. [H3] As a result, operators do not take actions or follow procedures specifically identified for handling dangerous goods.	Operators are not provided information regarding the true contents of a package or consignment. Operators do not observe or take special actions when consignments of batteries packed with or contained equipment display lithium battery marks but not hazard warning labels. Regulations are being applied in a manner beyond which they were intended. Changes in distribution system introduce potential for consolidation of many individual consignments. Each consignment is acceptable, but the consolidation of multiple packages in a mail sack is beyond the original intent of the Technical Instructions. Offerors are non-traditional dangerous goods personnel that only prepare lithium batteries/equipment. Regulations for shipping lithium batteries in the post do not support system constraints.

— END —