

太空事故調查與分類

彭鴻霖

2022-11-30

我國太空發展法與太空事故處理相關規定

我國太空發展法 (Space Development Act)

- 2021年6月16日公告。
- 第3條第一項第五款：
太空事故：指發射載具之發射過程中或太空載具運行過程中，所發生之故障、墜毀、碰撞或爆炸等事故。
Article 3
Space accidents: Malfunction, collapse, explosion and other accidents during the launch of a launch vehicle or operation of a spacecraft.
- 第18條：
太空事故之調查，由國家運輸安全調查委員會辦理。
Investigations into a space accident shall be conducted by Taiwan Transportation Safety Board

第四章 太空事故之處理

第 15 條

- 1 發射載具或太空載具之所有人或使用人，因故意或過失發生太空事故致人死傷，或毀損他人財物時，應負損害賠償責任。
- 2 太空活動涉及太空事故者，主管機關得令發射載具或太空載具之所有人或使用人限期改善；屆期未改善者，得令其中止計畫或廢止其發射許可。
- 3 前項限期改善之期限、中止計畫之事由、廢止許可及其他應遵行事項之辦法，由主管機關定之。

第 16 條

- 1 發射載具或太空載具之所有人及使用人，應於發射許可期間提供適當之責任保險或財務保證，並經主管機關核定，始得實施發射。
- 2 前項責任保險之保險人、發射載具或太空載具之所有人及使用人、財務保證之保證人，在保險或保證期間內，有停止、終止或變更其責任保險或財務保證之事由或內容者，應於六十日前以書面通知其他契約當事人。發射載具或太空載具之所有人及使用人應於通知其他契約當事人或收受通知之次日起三日內通知主管機關；未通知者，主管機關得依第十一條第三項所定辦法之規定廢止發射許可。

第 17 條

- 1 發射載具或太空載具之所有人或使用人，因太空事故發生損害賠償責任時，其最高限額為新臺幣五十億元，並得依前條責任保險或財務保證所取得之金額填補所造成之損失。
- 2 前項賠償限額，不包括利息及訴訟費用在內。
- 3 太空事故致生之損害，損害賠償請求權人如能證明係由發射載具或太空載具之所有人或使用人之故意或重大過失所致者，不受第一項賠償責任最高限額之限制。

第 18 條

太空事故之調查，由國家運輸安全調查委員會辦理。



國內太空活動概述

類別	國內狀況	備註 (國外案例)
民用發射載具	<p>一期計畫、二期計畫沒有案例。</p> <p>目前有飛鼠系列火箭，但是除供短期科研用途外，將以提供國際衛星市場發射服務並以境外發射為主，屬於發射載具所有人、設計人與設計國。</p>	<p>美國由主管機關 FAA 發許可證，NTSB 調查重大事故。</p>
公務發射載具	<p>一期、二期計畫的福衛系列衛星發射都是採外構發射服務合約，境外發射為主。探空火箭為二期計畫中主要計畫之一，由 NSPO 委託 CSIST 製造提供。</p> <p>三期計畫雖沒有探空火箭計畫，台灣聯合大學 (陽明交大為主) 與成功大學都有科研探空火箭計畫的規劃。</p> <p>預期三期計畫的衛星將循此模式進行。屬於發射載具的使用人或共同使用人。</p>	<p>美國太空科研計畫大多採購發射服務，使用民用發射載具。太空梭計畫由 NASA 主導調查事故 (mishap) 事件。</p>
民用太空載具	<p>立方衛星 / 低軌通訊衛星 / 合成孔徑衛星 (SAR)</p>	<p>美國由 FAA 發許可證，NTSB 調查重大事故。</p>
公務太空載具	<p>一期、二期福為系列衛星，三期計畫的自主任務型與研發型系列衛星。</p> <p>二期計畫由學校研發的立方衛星。</p> <p>中新通信衛星為太空載具共同所有人。</p> <p>CSIST 有可能發展合成孔徑衛星 (SAR) 或酬載，太空載具所有人、使用人。</p>	<p>美國科研部分由 NASA 各中心、JPL、NOAA 主導。NASA 總部調查重大事故。</p> <p>國防部分由 USAF 主導，DOD 調查重大事故。</p>
軍用太空載具	<p>有可能發展合成孔徑衛星 (SAR) 或酬載。</p> <p>太空載具所有人。</p>	<p>USAF DOD 調查重大事故</p>

國際太空活動與太空事故調查

國際太空活動相關機構/法規

- 聯合國外太空事務辦公室 (UNOOSA)
 - International Space Law: United Nations Instruments (2017)
 - Convention on International Liability for Damage Caused by Space Objects (1971)
- 聯合國和平利用外太空委員會 (COPUOS)
- 國際太空安全促進委員會 (IAASS)
- ICAO Annex 13, Aircraft Accident and Incident Investigation (擴充至商業太空飛行)

國外太空事故調查

- 美國
 - 美國 NASA (公務用)
NASA-PR-8621.1D:2020: 失常與虛驚 (mishap and close call) 通報、調查、與存檔程序
 - 美國 DoD (國防用)
DoDI 6055.07-C1:2018: 失常 (mishap) 通知、調查、報告、與存檔 (near miss)
 - NSTB (商業用)
- 英國
 - 2018年擬定太空法 (The Space Act)
 - 2021年7月, 英國航空事故調查局(UK Air Accidents Investigation Branch, AAIB) 被指定為英國太空事故調查主管機關 (SAIA)。
 - CAP 2219 (2021), 太空飛行事故調查指南

預防重於治療, 避免發生太空事故, 必須建立嚴謹的系統工程、安全管理, 以及全員風險思維與組織安全文化基礎!

太空事件：正常、...、異常、失效、虛驚、失常、失事、意外、事故、不幸、災難



事故分類案例：風險管理 ⇨ 危害分析與風險評鑑 ⇨ 後果嚴重程度

安全是指免於造成人員、財物、與環境的破壞後果！

Table 1 — Severity category definitions of identified hazards and consequences

Severity categories		Type of consequence	
1)	Catastrophic hazards	i)	Loss of life, life-threatening or permanently disabling injury or occupational illness, loss of an element of an interfacing manned flight system;
		ii)	Loss of launch site facilities or loss of system;
		iii)	Severe detrimental environmental effects;
2)	Critical hazards	i)	Temporarily disabling but not life-threatening injury, or temporary occupational illness;
		ii)	Major damage to flight systems or loss or major damage to ground facilities;
		iii)	Major damage to public or private property;
		iv)	Major detrimental environmental effects.
3)	Marginal hazards	Minor injury, minor disability, minor occupational illness, or minor system or environmental damage.	
4)	Negligible hazards	Less than minor injury, disability, occupational illness, or less than minor system or environmental damage.	

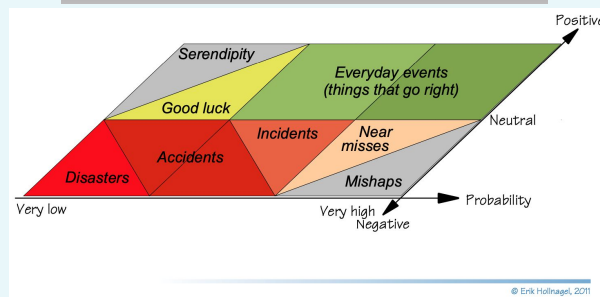
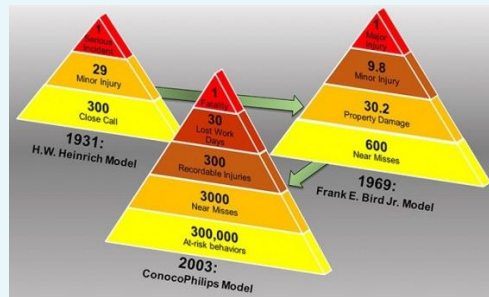
事故分類

事件 (event): 產品 ⇨ 合格、瑕疵; 任務 ⇨ 成功、失敗; 後果 ⇨ 安全、危險

危害 (hazard): 對人員、財物與環境的破壞。

- 人員: 致死 (fatality)、死亡 (death)、傷害 (injury)、疾病 (illness) (傷亡 = 傷害 + 死亡)
- 財物: 滅失 (loss)、損壞 (damange) (損失 = 損壞 + 滅失)
- 環境: 汙染 (contaminant)、破壞 (damage)

危安事件 (hazard event): 事故 (accident)、意外、不幸 (incident)、失事、失常 (mishap)、虛驚或未遂 (close call / near miss)



Heinrich (1931)	Bird (1969)	ConocoPhillips (2003)	DODI (2011) Mishap and Near Miss	NASA 8621.1D (2020) Mishap and Close Call
Major Injury	Fatal Accident	Fatality	Class A	Type A Mishap
Minor Injury	Serious Accidents	Lost Workday Cases	Class B	Type B Mishap
Incidents (Near Miss)	Accidents	Recordable Injuries	Class C	Type C Mishap
	Incident	Near Misses	Class D	Type D Mishap
		At-Risk Behaviors	Class E	Close Call
			Class F	

風險管理 ⇨ 風險圖像 ⇨ 嚴重程度 ⇨ 事故分類與分級案例

風險圖像

Medium	High	Very High	Severe	Severe	Severe
Medium/Low	Medium	High	Very High	Severe	Severe
Low	Medium/Low	Medium	High	Very High	Severe
Low	Low	Medium/Low	Medium	High	Very High
Low	Low	Low	Medium/Low	Medium	High
	< 0.0001 per year	Low	Medium/Low	Medium	
		< 0.00001 per year	Low	Medium/Low	
			< 0.000001 per year	Low	

後果分級



Description & Category	Actual or Potential Occurrence	Effect To People			Effect to Asset		Effect to Environment
		1 st Parties	2 nd Parties	3 rd Parties	Human Rated	Unmanned	
Catastrophic	Accident	More than one 1 st Party deaths (for 2 or more flight crew); single death for single pilot operations	Multiple 2 nd Party deaths	One or more 3 rd Party death	Loss of spacecraft	Loss of spacecraft as unable to continue safe flight and landing	Extreme widespread environmental damage
Hazardous	Serious Incident - Asset or Accident (people death)	Single 1 st Party death (for 2 or more flight crew); serious injury (single pilot ops) ; or excessive workload impairs ability to perform tasks	Single 2 nd Party death	Serious injuries to more than one 3 rd Party	Severe damage to spacecraft Large reduction in Functional capabilities or safety margins	Loss of spacecraft due to controlled (directed) termination over unpopulated emergency site	Severe environmental damage
Major	Major Incident	Serious injuries/ illnesses to 1 st Parties (for 2 or more flight crew); minor injury (single pilot ops) ; Physical discomfort or a significant increase in workload	Serious injuries/ illnesses to 2 nd Parties Physical discomfort	Serious injury to a single 3 rd Party	Major damage to spacecraft Significant reduction in functional capabilities or safety margins	Severe damage to spacecraft Large reduction in Functional capabilities or safety margins	Major environmental damage
Minor	Minor Incident	Minor injuries/illnesses to 1 st Parties (for 2 or more flight crew); serious injury (single pilot ops) ; Slight increase in workload	Minor injuries/illnesses to 2 nd Parties	Minor injuries to more than one 3 rd Party	Minor damage to spacecraft Slight reduction in functional capabilities or safety margins	Major damage to spacecraft Significant reduction in functional capabilities or safety margins	Minor environmental damage
Negligible	Occurrence without safety effect	Inconvenience	Inconvenience	Minor injury to a single 3 rd Party	Less than Minor damage system	Minor damage to spacecraft Slight reduction in functional capabilities or safety margins	Less than minor environmental damage

Table 2: Severity Classifications

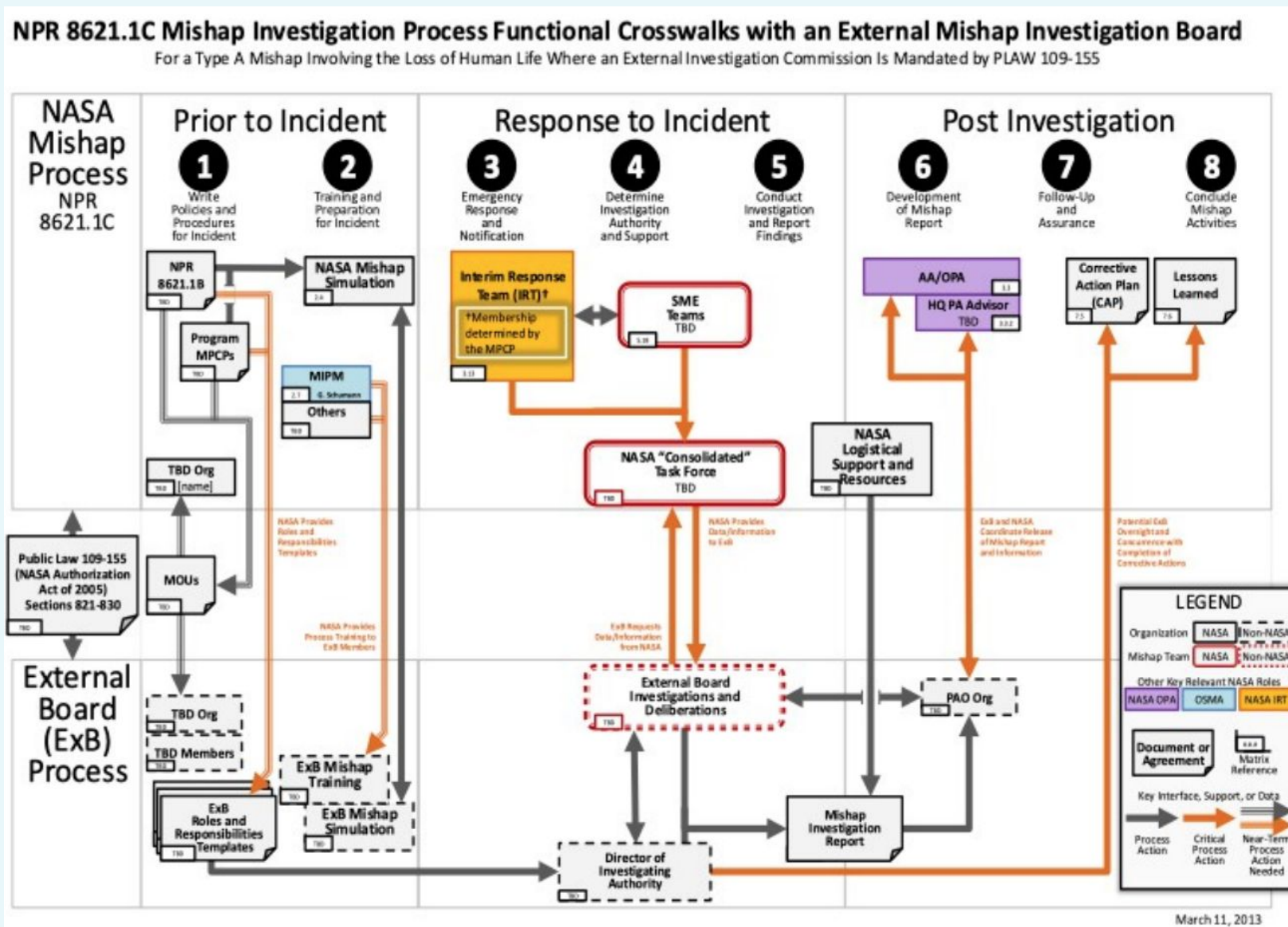


太空事故調查分工合作建議 (參與團隊與工作小組)

- 適切的安全分析與建檔，呈現關鍵潛在過程缺失與根本原因 (safety cases)，第一次就沒有犯錯，不是下一次不會犯錯！
- 所有違安事件 (unsafety or hazard event)，包括事故或重大意外 (accident or fatality)、意外 (incident)、與虛驚 (near miss or close call) 三大類，所有人及(或)使用人負完全責任。
- 運輸安全調查法是澄清事故真因的法令，當然包括所有太空運輸安全與違安事件，明定運安會與太空活動主管機關之調查職責分工。
- 重大事故調查作業規則由運安會相關程序制定，重大事故以外事件之調查程序由主管機關自行訂定。

- 事故或重大意外 (accident or serious incident) (unplanned): 故意(蓄意)或過失，明知不可為而為之，包括死亡與五人以上重大傷害，或發生傷亡之重大意外，由獨立機關運安會負責調查。
- 意外或一般事故 (incident) (undesired): 善盡職責仍然發生、意料之外簡稱意外，由太空活動主管機關負責調查，結果送運安會備查。
- 虛驚 (near miss or close call): 有驚無險，由太空載具或太空載具之所有人或使用人管理階層負責調查，結果送主管機關備查。

NASA 失事調查過程 ⇨ TTSB 既有調查作法大致符合 ⇨ 應用與落實



太空運輸安全依賴太空系統安全與產品保證 → 以終為始、從頭做起！

• 運輸載具

- 軌道車輛 (railway rolling stock)
- 道路車輛 (road vehicles) 與道路交通 (Road Traffic) 有所區別。
- 自動車 (automotive) (汽油車、柴油車、電動車)、車用積體電路、機車 (摩托車), 農業用車、特殊用途車輛、...
- 水路運輸:
- 海路運輸:
- 航空運輸: 民航機、直升機、無人機、...
- 發射載具: 入軌火箭、探空火箭
- 太空載具: 人造衛星、太空船(載人、無人)

• 人員、財物、環境都一樣、只是載具改！

• 凡走過留下透明可信的事件因果鏈軌跡！

• 要有冒險犯難的精神、不能有違規犯法的企圖！

安全範疇: 人安、物安、資安

安全理念: 安全共好、事故共業、平台共用、資訊共享

安全管控: 平時檢查、管理審查、治理稽核、事後調查

安全對策: 事前預防、臨前檢查、事中調適、臨後改正、事後更新

讓運安會只做建立國外經驗學習案例, 提供國內太空活動玩家借鏡！

Model-Based Systems Engineering

Evidence-Based Product Assurance

Agile, Adaptive Mission Assurance

Risk-Informed Safety Case

ALARP (合理務實風險) vs. ASARP (合理務實安全)

• 產品安全性 (product safety)

- 安全功能安全 (functional safety): ISO 26262
 - 意圖功能安全 (intended function safety): ISO 21448
 - 網路資訊安全 (cybersecurity): ISO/IEC 27001, ISO/IEC 27001, ISO/SAE 21434
 - 管理系統: IAQG 9100 (航太)、ISO/TS 22163 (IRIS) (軌道車輛)、IATF 16949 (自動車)
 - 工作安全: ISO 45001 (職安)、ISO 39001 (路安)
- 系統工程過程: 需求管理、系設計與發展、先進產品以終為始、品質規劃、成熟度等級評鑑、失效模式與效應分析; 危害與威脅分析、風險評鑑、應變規劃、韌性管理。
- 系統 + 過程: 掌握「金、人、事、時、地、物、場」流動, 採取 PDCA 滾動式持續改進。
- 實證: 紀錄、資料庫、大數據, 統計、機率、人工智慧。
- 從程序書 + 紀錄, 到文件, 到建檔資訊。
- 從紙本, 到電子數位, 到電腦, 到網路。
- 文件管理、變更管理、資訊管理、知識管理, 型態管理。



安全管制 ⇨ 功能安全管理 + 系統安全管理 ⇨ 韌性管理

• 管理作業活動

- 安全性政策
- 安全性文化
- 安全性過程
- 安全性手法
- 訓練與資格鑑定

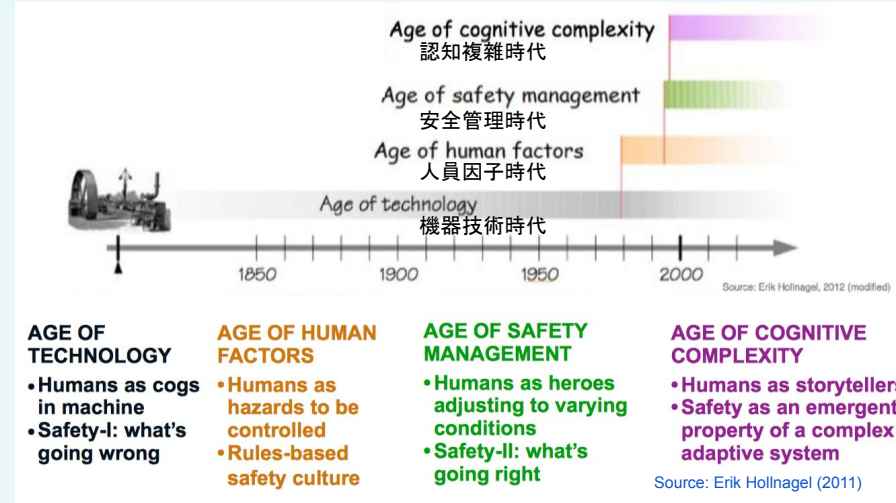
• 創新與變更

- 安全性經理
- 安全核心團隊
- 變更控制委員會

• 安全 I + 安全 II + 安全 III

- 安全 I: 設備安全 (Dr. Taylor)
- 安全 II: 工作安全 (Dr. Hollnagel)
- 安全 III: 系統安全 (Dr. Leveson)

安全思維演進



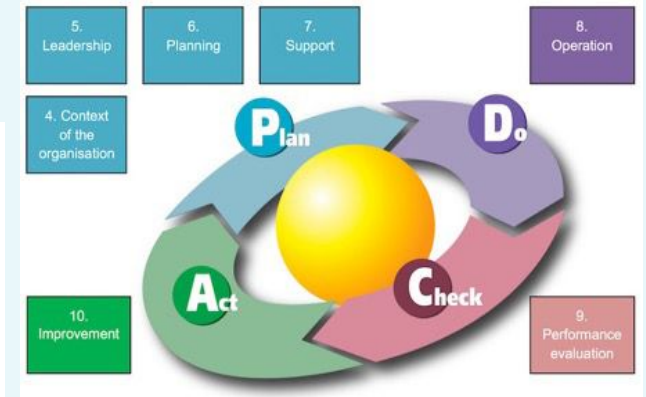
• 安全管理計畫

- 目標: 系統性規劃所有安全相關作業活動, 累積作為安全案例的基礎。
- 內容: 職責分工, 研發過程規劃、避免錯誤或故障的程序與手法, 所使用的發展工具, 記錄與報告 (安全案例)。
- 手法: 被動、裁適、預測、互動、自動、主動、自主、調適 (reactive, tailor, predictive, interactive, automatic, proactive, autonomous, adaptive)

Unknown Unknown & Unpredictable!

東西不好、任務失效, 可能發生危害、傷亡。
東西好、任務成功, 但也會發生危害、傷亡!

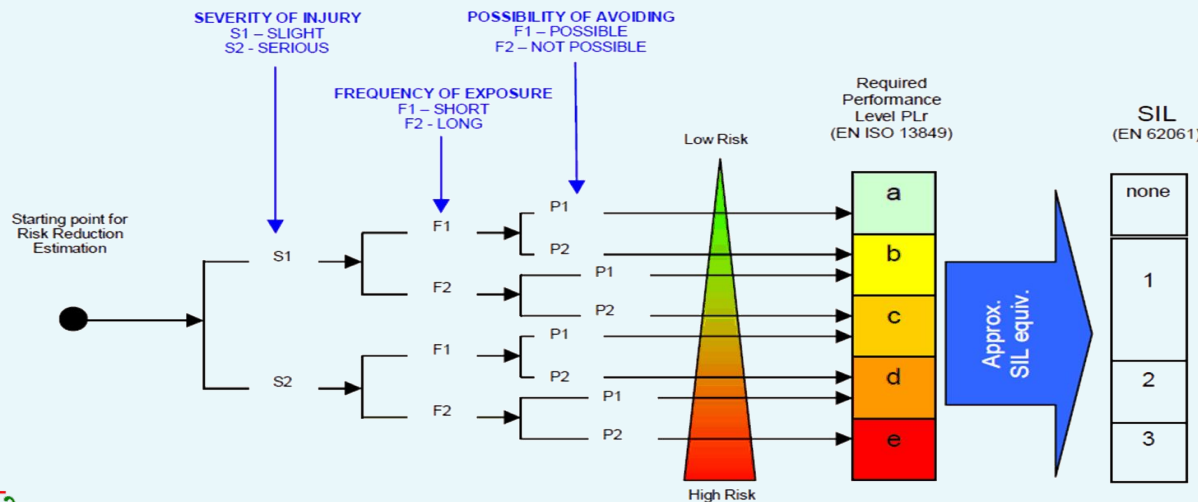
ISO 管理系統標準高階架構 (MSS HLS)



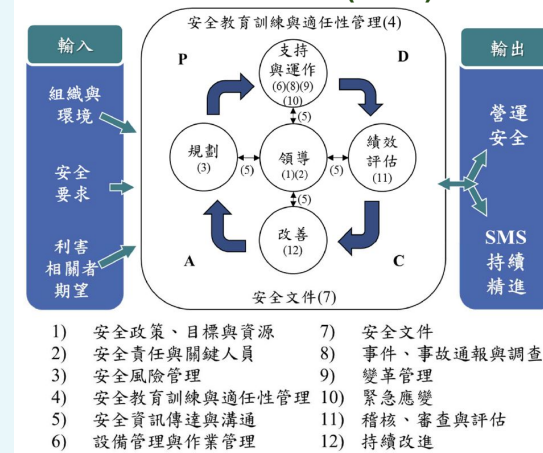
MIL-STD-882 ⇨ ISO 21448 (SOTIF)、ISO/SAE 21434 (Cybersecurity)

EN 954 ⇨ ISO 13849 ⇨ IEC 62021

IEC 61508 ⇨ ISO 26262、EN 50156、IEC 61511、IEC 61513...



安全管理系統 (SMS)



Don't do it that way!



發展太空產業 ⇨ 安全與任務成功兼顧 ⇨ 太空標準與異業融合

ISO/TC 20/SC 14
Space systems and Operations

ESA ECSS: Standards, Handbooks & TMs
<https://ecss.nl/standards/>

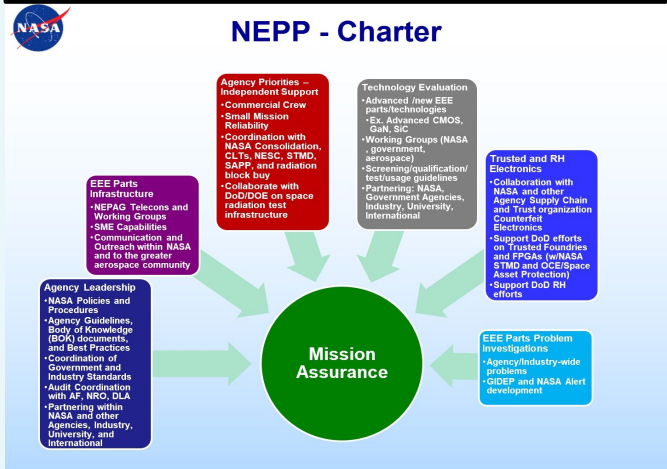


The European Cooperation for Space Standardization (ECSS) is an initiative established to develop a coherent, single set of user-friendly standards for use in all European space activities

NASA + ESA + JAXA TRISMAC
Trilateral Safety and Mission Assurance Conference



NASA NEPP Parts and Packaging Program (ETW)
<https://nepp.nasa.gov/workshops/etw2022/talks/index.html>



https://nepp.nasa.gov/images/program/nepp_charter.jpg

ITAR Free EEE Parts
MEWS Microelectronics Workshop
<https://ssl.tksc.jaxa.jp/mews/en/index.html?top>

日本 JAXA 電子零件網站:
<https://eeepitnl.tksc.jaxa.jp/en/info/history.htm>

陸地與太空環境比較

Spacecrafts	Automobiles
<p>◆ National space development project</p> <p><Demands for components></p> <p>Q: Ensuring absolute quality</p> <p>C: Enormous cost for component development</p> <p>D: Taking time to develop components</p> <p>{ H-II rocket: 19 billion yen } { H-IIA rocket: 9 billion yen }</p>	<p>◆ General-use</p> <p><Demands for components></p> <p>Q: Ensuring high reliability (Car carries human lives.)</p> <p>C: Limited expense</p> <p>D: Developing components to meet car release schedule</p> <p>Car is a high-volume product for general users and carries human lives.</p>

車用與家用環境比較

Automobiles	Household appliances
<p>• High/low temperature, moisture</p> <p>• Vibration, shock</p> <p>• Dust, rain, saltwater etc.</p>	<p>• Air-conditioned room</p> <p>• No vibration</p> <p>• No dust, no wetting</p>

High reliability demand ⇒ Automobiles must endure harsh environments.



國際太空安全管理相關規範 (冰山一角)

國際標準化組織 (ISO) 太空系統系列安全相關國際標準 (針對國際太空站、低軌衛星、立方衛星, 以 EAS ECSS 為藍本)

- ISO 11231:2019, Space systems - Probabilistic risk assessment (PRA)
- ISO 14620-1:2018, Space systems - Safety requirements - Part 1: Systems safety
- ISO 14620-2:2019, Space systems - Safety requirements - Part 2: Launch site operations
- ISO 14620-3:2021, Space systems - Safety requirements - Part 3: Flight safety systems
- ISO 17400:2021, Space systems - Space launch complexes, integration sites and other facilities - General testing guidelines
- ISO 17666:2016, Space systems - Risk management
- ISO 17770:2017, Space systems - Cube satellites
- ISO 21980:2020, Space systems - Evaluation of radiation effects on Commercial-Off-The-Shelf (COTS) parts for use on low-orbit satellite
- etc.

ICAO

- ICAO-9859:2018-ed4.0, Safety Management Manual
- ICAO Anex 13:2016-ed11.0, Aircraft Accident and Incident Investigation
- ICAO-D-9156:1997-ed2.0, Accident / Incident Reporting Manual

太空產業安全管理參考文件

- NASA/SP-2016-6105-Rev 2, NASA Systems Engineering Handbook
- NASA/SP-2010-580, NASA System Safety Handbook, Volume 1: System Safety Framework and Concepts for Implementation
- NASA/SP-2014-612, NASA System Safety Handbook, Volume 2: System Safety Concepts, Guidelines, and Implementation Examples
- FAA Flight Safety Analysis Handbook, Version 1.0, 2011
- JERG-1-007E, Safety Regulation for Launch Site Operation, JAXA, 2019
- CAP 2219, Guidance on the Investigation of Spaceflight Accidents, UK
- NASA-PR-8621.1D:2020, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigation, and Recordkeeping
- DoDI-6055.07-C1:2018, Mishap Notification, Investigation, Reporting, and Record Keeping
- CAP-2215, Guidance for the Assessment of Environmental Effects (AEE), 2021, UK
- CAP-2219, Guidance on the Investigation of Spaceflight Accident, 2021, UK
- AFSPCMAN 91-710 series, Range Safety User Requirements Manual
- etc.



謝謝聆聽
敬請指教

