淺談汽車領域的安全三連：Safety 、Security 和 SOTIF (1)

以下原文源於 20211130 EDN TAIWAN 電子報

功能安全(Functional Safety，FuSa)，資訊安全(Cybersecurity)和預期功能安全(Safety of the Intended Functionality，SOTIF)是今天談到汽車安全必須提的三個話題。

功能安全(Functional Safety，FuSa)，資訊安全(Cybersecurity)和預期功能安全(Safety of the Intended Functionality，SOTIF)是今天談到汽車安全必須提的三個話題。10 年前我在讀大學時做過部份關於汽車 Security 的工作，FuSa 則是跟著公司做過一系列培訓，在具體工作中對 Security 和 FuSa 都有接觸。而 SOTIF 則比較新，是一個汽車安全領域針對智慧化的新興話題。這幾個安全話題彼此不同又相互關聯，這裡我想簡單地梳理它們之間的關係和範疇。

「道路千萬條，安全第一條。」——電影《流浪地球 2》都開拍了，這個梗也是老梗了，但是道理並不過時。這裡的安全指的是駕駛員的操作安全，既不是 FuSa，也不是 Cybersecurity 的安全範疇，而是更貼近於 SOTIF 預期功能安全的誤用(misuse)內容。安全是一個比較廣泛宏觀的概念，同時也是一個相對的概念。剛開始接觸安全話題時，大學教授對我們說的第一句話就是「沒有百分之一百的安全，一切都是相對的」。汽車安全是安全領域的一個細分，和傳統的電腦，金融方向的安全話題對比，有很多類似的地方，但也有其特殊的一

面。汽車產業的產品安全工程是一個跨領域、系統化的過程，需要相關部門密切交流協作才能達到預期的安全目標。

Vector 日前舉辦汽車安全研討會(A Big Success — 4th Automotive Cybersecurity Symposium)，探討與汽車攸關的 'Safety' 和 'Security' 等安全議題。

以英文來看， 'Safety' 可以簡單地看成由機器造成的安全問題，而 'Security' 則是指由惡意者比如駭客造成的安全問題。可是翻成中文，這兩個詞的意思都是「安全」，這就尷尬了，其實同樣的問題也發生在德語裡，德語也是只有一個 Sicherheit 來指代「安全」，所以當我們在表述汽車安全時，不是要搬出英語來，就是要加上首碼。德國公司把功能安全有時候稱為 'FuSa' ，有時又稱為 'FuSi' (德語版，感覺好聽點)，也是個薛丁格的安全。中文傾向把 Cybersecurity 翻譯成資訊安全，德語也經常加資訊的首碼，不知道是誰影響的誰。但這麼翻譯其實凸顯不出背後的人為因素，看到某乎上

安全達人博主殷瑋說最好叫防護安全，我覺得這樣更加貼合，或者叫防禦安全，把人的因素表現出來。

那麼，‘FuSa’和‘SOTIF’又有什麼區別？我的理解是，FuSa 針對的是機器出問題了，汽車說我出故障(Malfunction)了，造成安全問題，靠冗餘可以解決。而 SOTIF 則指的是汽車系統沒出問題，只是功能不夠，或者操作不當，造成功能安全問題了，是汽車說臣妾做不到，冗餘也解決不了。SOTIF 更主要的是針對輔助駕駛和自動駕駛而言。比如，感測器並沒出問題，但是沒辨識出人和障礙物，撞上去了，或者是人把礦泉水瓶別在方向盤上騙過汽車，汽車以為你在單手操把，這都是 SOTIF 的範疇。最早特斯拉(Tesla)沒辨識出白色卡車撞上去，和 Uber 的車撞人，都在 SOTIF 的範圍內。SOFIT 可以理解是為了因應汽車智慧時代的到來，填補了‘FuSa’不能應對的空白。

理論上，一個產品只有在可以預期預料的使用中不會對人的健康和安全造成風險的時候才可以投入市場。但問題是，如何衡量？是否能定量地衡量？還是得依靠專業經驗去衡量。這也使得相應的標準和法規尤為重要。

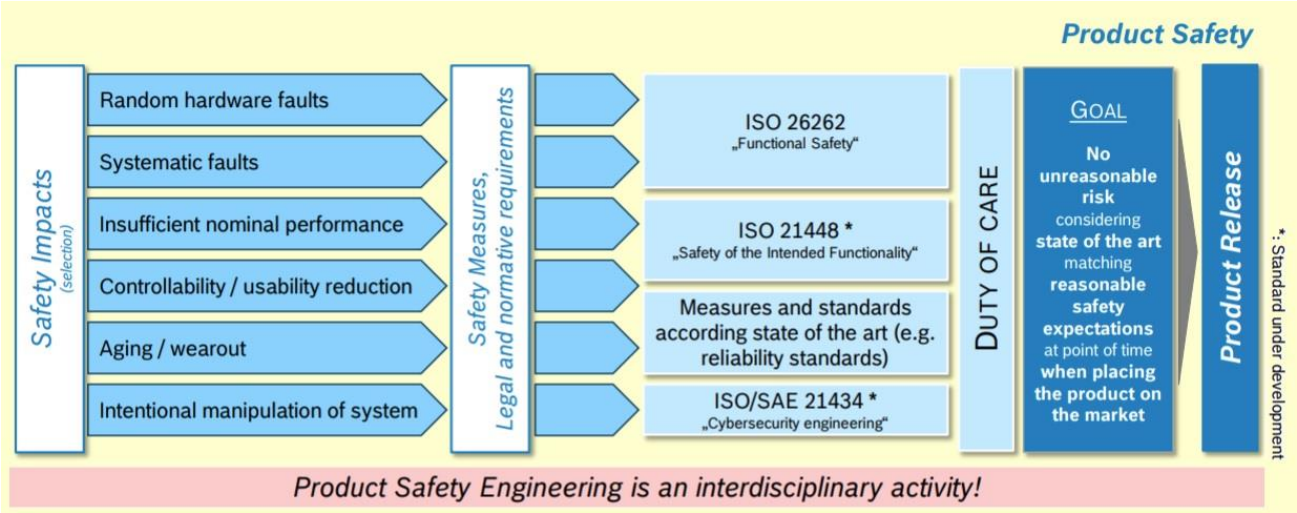

圖 1：跨領域、系統化的汽車產品安全。(來源：Vector Automotive Cybersecurity Symposium)

最近看網上維克多(Vector)的第四屆汽車安全研討會(Automotive Cybersecurity Symposium)，有不少德國整車廠和供應商專家的報告，大家有興趣可以去看看。**圖 1** 源自博世(Bosch)安全專家 Stefan Kriso 的講稿。從安全分析到產品發佈，這是一個系統化的過程，涉及一系列的措施，也涉及一系列的標準。像針對 ‘FuSa’ 的 ISO26262 (2011 年 11 月發佈)，尚在開發中針對 SOTIF 的 ISO21448 (2022 年 3 月發佈)和針對 Cybersecurity 的 ISO21434 (今年 8 月底發佈)，所以說汽車安全工程也是一個跨領域的過程。對於 FuSa 而言，傳統車企內部一般有安全中心，每個團隊一般也有自己的安全專家，很多團隊內的安全專家都有在安全中心工作的經驗。我所在部門的安全專家就是這樣既對部門的全域非常瞭解，能獨當一面，又有非常強的跨部門合作能力。各部門協調分析，明確職責，才能共同實現安全目標到產品發佈。

從這三個標準的發佈可以看出，ISO26262 已經馬上 10 歲了，ISO21434 才剛一個多月，而 ISO21448 仍然在開發過程中。所以，相應的 FuSa 流程已經很成熟，而後面兩個標準聽到的次數要少很多。傳統車企已經積累了很多 FuSa 相關的經驗和方法論，這些經驗和方法論是否適用於另外兩種年輕的標準呢？

還是從 ISO26262 說起。說起 FuSa，必然要說到危害分析和風險評估(Hazard Analysis and Risk Assessment，HARA)和車輛安全完整性等級(Automotive Safety Integrity Level，ASIL)，可以透過清楚的公式和列表來進行風險評估分析。前面已經提到，FuSa 是針對汽車本身出故障的，沒有人為因素，其實是個統計學問題。駕駛時長和故障率是相互獨立的統計學事件，時間到了，不管哪輛車，故障是按概率來發生，而不以人的意志為轉移。而轉到 Cybersecurity 的話題，這個大背景前提就發生了變化，駭客是否攻擊你的車是有意識的，和駕駛情況不再是統計學獨立的了。比如王胖子和胡八一都買一樣的車，駭客可能盯著王胖子的車黑，而完全不去黑胡八一的車。這就使依賴於統計獨立性的 ASIL 對 Cybersecurity 不再適用。但這也並不等於說 ISO21434 和相應的威脅分析和風險評估(Threat Analysis and Risk Assessment，TARA)完全要從零開始另起爐灶，它的過程有部分還是借鑒了 HARA 的過程，也借鑒了傳統電腦安全領域的標準，比如通用評估準則(Common Criteria，CC)。

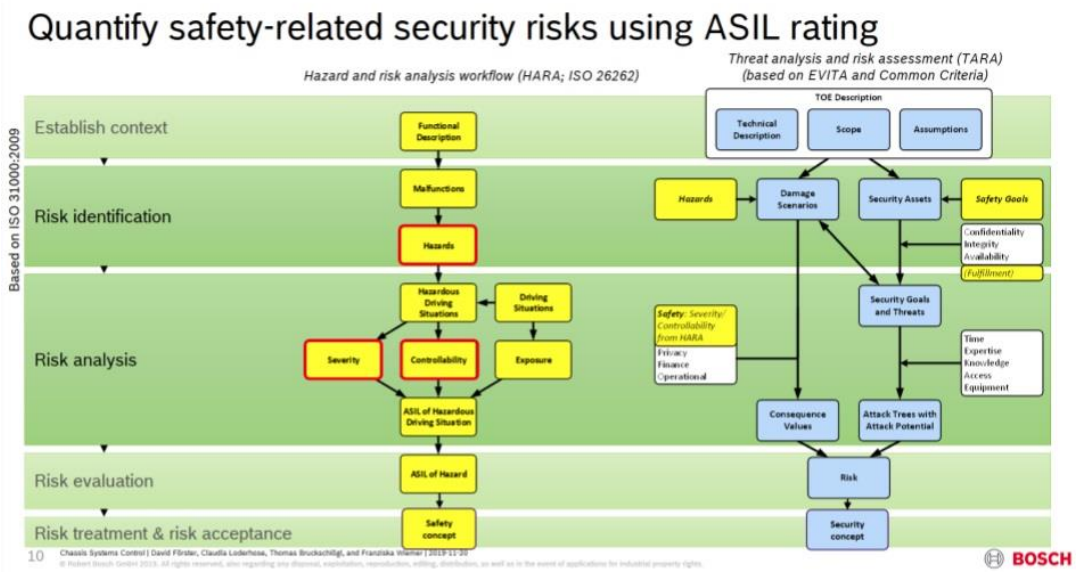

圖 2：博世公司的 TARA 過程。(來源：Vector Automotive Cybersecurity Symposium)

博世給出的 TARA 方案如**圖 2** 所示。和 CC 類似，基於統計學的內容基本消失了，更多的是基於場景、經驗和知識的評估。Safety 和 Security 在出問題時造成的危害、嚴重性、可操控性，以及想要達到的安全目標，這幾部份是相通的(見圖中的星號標註)，所以可以借鑒。在資訊安全或者防禦安全領域的 CIA (保密性、完整性、有效性)上，汽車產業的 Security 和傳統電信產業的 Security 也是相通的(見圖中三角標註)，所以也能借鑒。TARA 也是站在既有標準的肩膀上起步的。

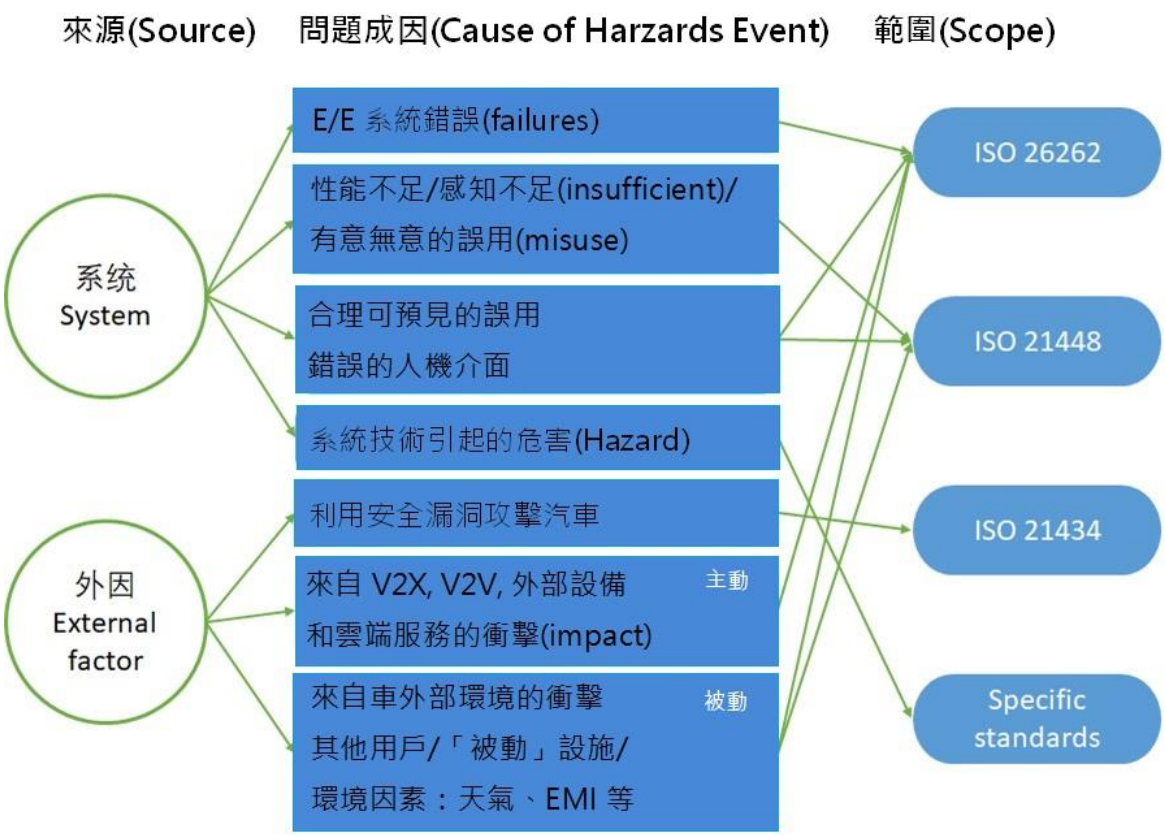

圖 3：ISO21448 中安全相關話題與 ISO 標準的關聯總覽。

說了這麼多，那麼到底如何界定一個問題隸屬於哪個或者哪幾個標準的範疇呢？博世同樣給出了從系統內因外因，以及問題產生的成因來確定問題隸屬範圍的界定。看完會發現並不是像第一印象那樣所有外部因素造成的問題都屬於 Security 的範疇，也有可能是 SOTIF 或 FuSa。ISO21448 中闡述了**圖 3** 中的分類，可以把它作為一個基礎去理解與之相應的這三種安全話題。好多問題其實都涵蓋了幾種成因，也可以落實在不同的 ISO 標準範疇內。

圖 4：被污染的交通標誌。(來源：https：//winfuture.de/news,99034.html)

比如，被塗鴉或者污染的交通指示牌(如**圖 4**)，可能會造成汽車視覺系統辨識錯誤，這種就屬於 SOTIF 的範疇。而如果遇到有人用投影儀投一個逼真的虛擬指示牌在路邊牆上，汽車視覺系統辨識之後也可能會產生安全問題，這就不再是 SOTIF 的範疇，而是 Security 的範疇了。

還是那句話，道路千萬條，安全第一條。不管是按照標準穩紮穩打的傳統車企，還是繞開標準做法激進的某些新興車企，安全是所有人繞不開的話題。智慧化的汽車到底有多安全？佔據各大頭條的某些新聞，到底是汽車安全事故還是一場鬧劇？關於汽車安全的爭論此起彼伏，莫衷一是，但是兩點是肯定的：如果不重視汽車安全，墨菲定律會不斷應驗，「親人兩行淚」還會繼續發生；但同時，過份追求安全也可能變成一套銬住傳統車企的枷鎖，讓它在面對激進的新興車企的競爭時更加壓力重重。

安全，是把雙刃劍.....

編按：在汽車安全領域，如何提高安全也要能文能武，在介紹這三方各自的定義和範疇及其相互關聯後，後續報導將結合實際場景深入分析，請繼續閱讀「*淺談汽車領域的安全三連：Safety、Security 和 SOTIF (2)*」