

2024  
DevOps Tec. x SIEMENS  
POLARION

# Polarion ALM x Cybersecurity : 安規與企業流程最佳實踐

Jason – DevOps Tec.

合辦單位：



SIEMENS



個人經歷介紹

## Background



Jason Xue 薛家丞

戴博斯科技股份有限公司 – 工程部工程師

專精於Polarion ALM系統的企業導入以及企業專案管理系統的整合規劃。  
經驗涵蓋電子、軟體、資訊和金融產業。擅長系統分析、設計，與系統客  
製化開發。曾服務友達光電、中磊電子、智易科技等客戶。

目錄概要

# Outline

01 What is ISO21434

04 風險管理與漏洞追蹤

02 Automotive cybersecurity x  
Polarion ALM

05 監控和持續改進

03 安全需求管理

06 Polarion X



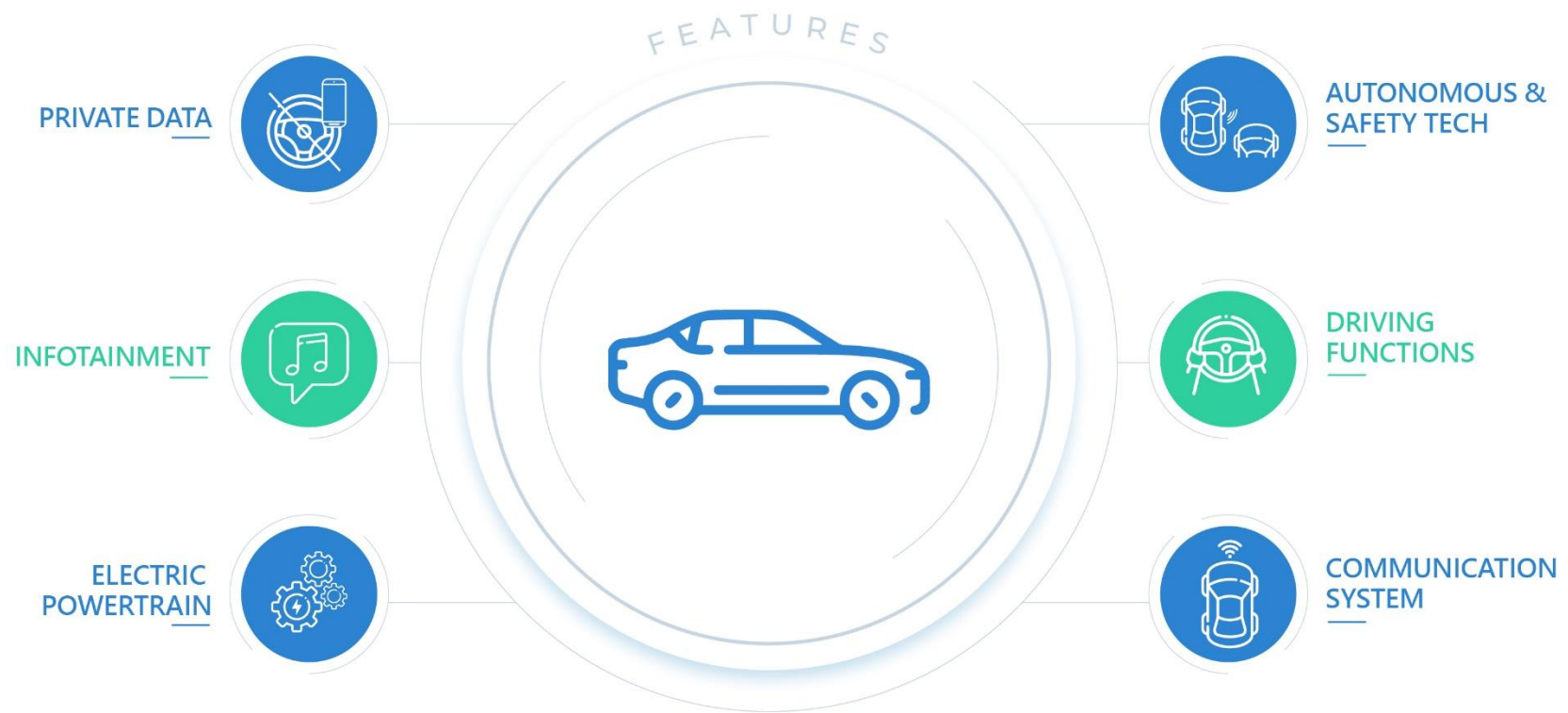
01

# What is ISO21434



# What is ISO21434

在車聯網的發展趨勢之下，網路安全的風險成無法迴避的挑戰，如何讓現今的汽車製造商與供應商能符合網路安全風險管理要求，ISO/SAE 21434標準受極大關注





# What is ISO21434

駭客有可能透過資安漏洞進行網路安全攻擊，  
過往的 ISO 26262 主要專注於汽車電子系統的功能安全性，並未對車輛網路安全進行規範。

## 車輛網路安全ISO/SAE 21434 標準出爐， 確保產業從設計開始就考慮潛在威脅

The screenshot shows the ISO/SAE 21434:2021 document page. The table of contents is as follows:

4. General considerations													
5. Organisational cybersecurity management													
5.4.1 Cybersecurity governance	5.4.2 Cybersecurity culture	5.4.3 Information sharing	5.4.4 Management systems	5.4.5 Tool management	5.4.6 Information security management	5.4.7 Organisational cybersecurity audit							
6. Project dependent cybersecurity management													
6.4.1 Cybersecurity responsibilities	6.4.2 Cybersecurity planning	6.4.3 Tailoring	6.4.4 Reuse	6.4.5 Component out-of-context	6.4.6 Off-the-shelf component	6.4.7 Cybersecurity case	6.4.8 Cybersecurity assessment	6.4.9 Release for post-development					
7. Distributed cybersecurity activities													
7.4.1 Supplier capability		7.4.2 Request for quotation			7.4.3 Alignment of responsibilities								
8. Continual cybersecurity activities													
8.3 Cybersecurity monitoring		8.4 Cybersecurity event evaluation		8.5 Vulnerability analysis		8.6 Vulnerability management							
9. Concept phase			10. Product development phase		11. Cybersecurity validation		12. Production						
9.3 Item definition			10.4.1 Design		11.1 Cybersecurity validation		12.3 Cybersecurity incident response						
9.4 Cybersecurity goals			10.4.2 Integration and verification				12.4 Updates						
9.5 Cybersecurity concept							13.3 Cybersecurity incident response						
							13.4 Updates						
14. End of cybersecurity support and decommissioning													
15. Threat analysis and risk assessment methods													
15.3 Asset identification		15.4 Threat scenario identification		15.5 Impact rating		15.6 Attack path analysis		15.7 Attack feasibility rating		15.8 Risk value determination		15.9 Risk treatment decision	

**ABSTRACT** [PREVIEW](#)

This document specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

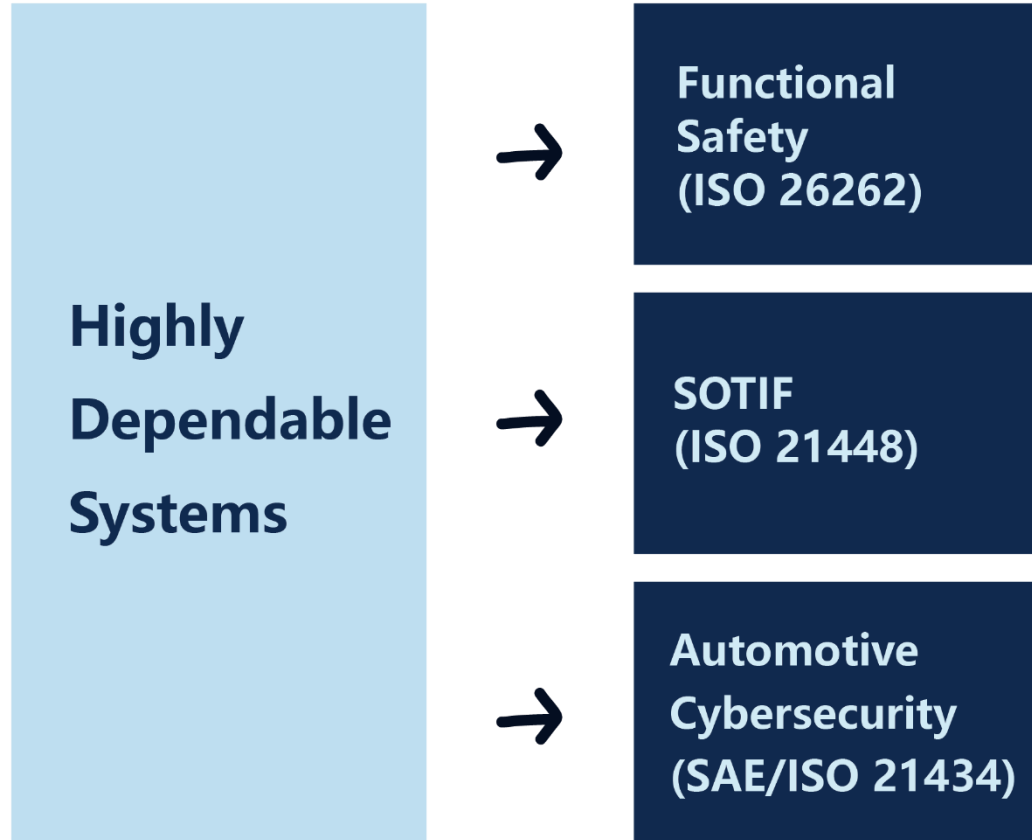
A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their



# What is ISO21434

ISO 26262主要關注汽車電子系統的功能安全性，而ISO 21434則專注於車輛系統的軟體安全性。

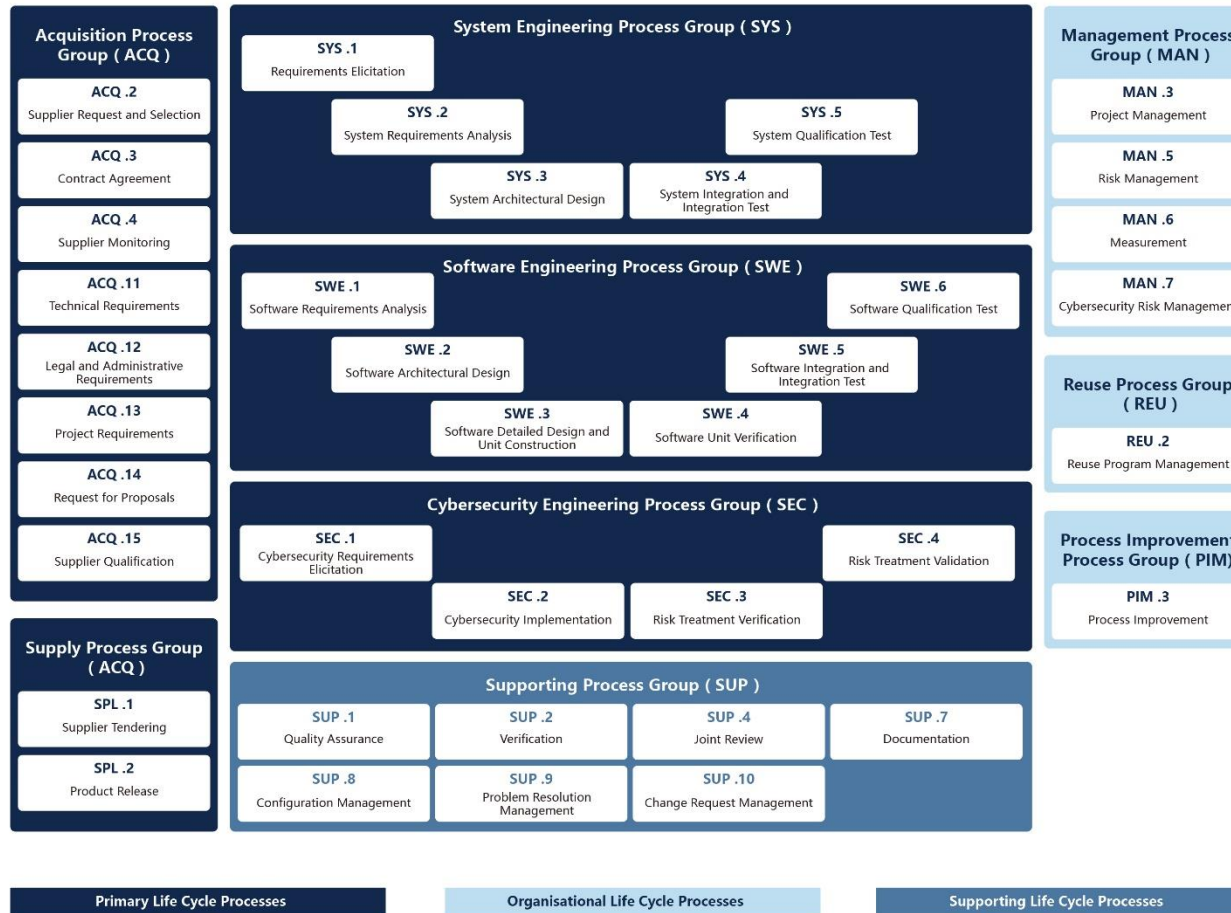




# What is ISO21434

ASPICE V-Model 中 SEC.1-4 為 ISO21434 規範範圍

## Automotive SPICE V - model - Overview





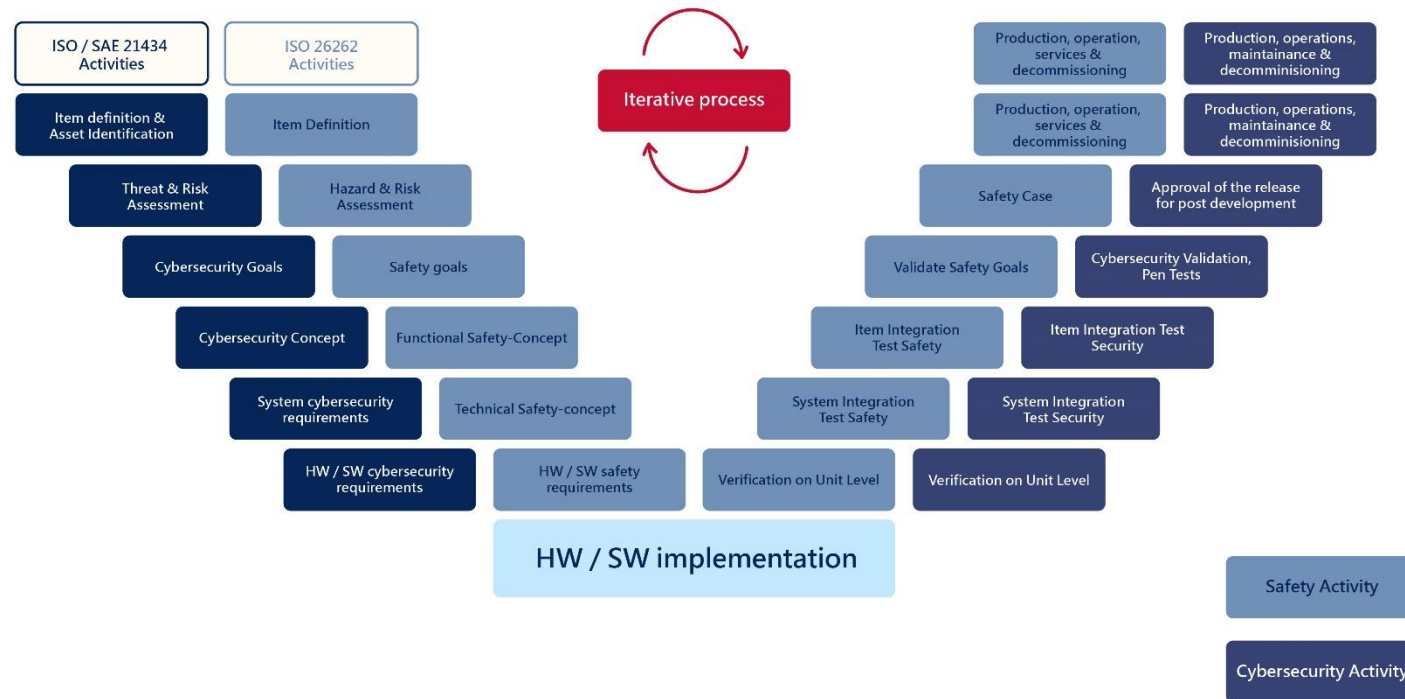
# Automotive cybersecurity x Polarion ALM

我們將依照 安全需求管理-> 風險管理與漏洞追蹤(驗證) -> 監控和持續改進  
的流程為各位介紹如何在 Polarion ALM 實踐 Cybersecurity



# Automotive cybersecurity x Polarion ALM

ASPICE V-Model 中加入 ISO21434 規範後我們可以看到，在各階會有相對應的 Cybersecurity 工作項目產生，並且與原先 ISO26262 產品生命週期平行，接下來我們將已實際案例作為例子。介紹當我們使用 Polarion ALM 在產品生命週期中加入 Cybersecurity 後會造成怎樣的影響與改變。



02


# Automotive cybersecurity x Polarion ALM

實際案例

# Automotive cybersecurity x Polarion ALM


可以從 Dashboard 上看到 Cybersecurity 總覽，如前面所述接下來將使用 ISO-664 User Interface for GPS based navigation system 為舉例。

## Item View







Item:  ISO-664 - User Interface for GPS based navigation system

Item responsible: System Administrator

[Select Another Item](#)











Status:  In Analysis

### Document Overview

Document	Status	Type	Author
 User Interface for GPS based navigation system - 1.0 - Cybersecurity Plan	 Draft	 Cybersecurity Plan	System Administrator
 User Interface for GPS based navigation system - 1.0 - Cybersecurity Case	 Draft	 Cybersecurity Case	System Administrator

### Asset Overview

[Manage Assets](#)

Asset	Status	Assignee
 ISO-683 - I/F for entering data on in-vehicle device	 Open	
 ISO-684 - I/F to speech recognition system	 Open	
 ISO-681 - USB Controller	 Open	
 ISO-682 - Wlan connection for mobile app	 Open	
 ISO-680 - Message broker	 Open	

# Automotive cybersecurity x Polarion ALM

並介紹如何規劃包含 Risks , Threat Scenarios ,Damage Scenarios , 並產生報表 , 確保所有的風險都已經過驗證。

### Risks

🔗 Manage Attack Paths & Risks

Risk	Status	Assignee	Risk Severity	Risk Treatment	Goal/Claim
🔗 ISO-690 - Risk of disclosing target data	Draft		<span style="background-color: #800000; color: white; padding: 2px;">S</span> <span style="background-color: #800000; color: white; padding: 2px;">F</span> <span style="background-color: #800000; color: white; padding: 2px;">O</span> <span style="background-color: #800000; color: white; padding: 2px;">P</span>	Retaining the risk	⚠️

### Threat Scenarios

🚗 Manage Threat Scenarios

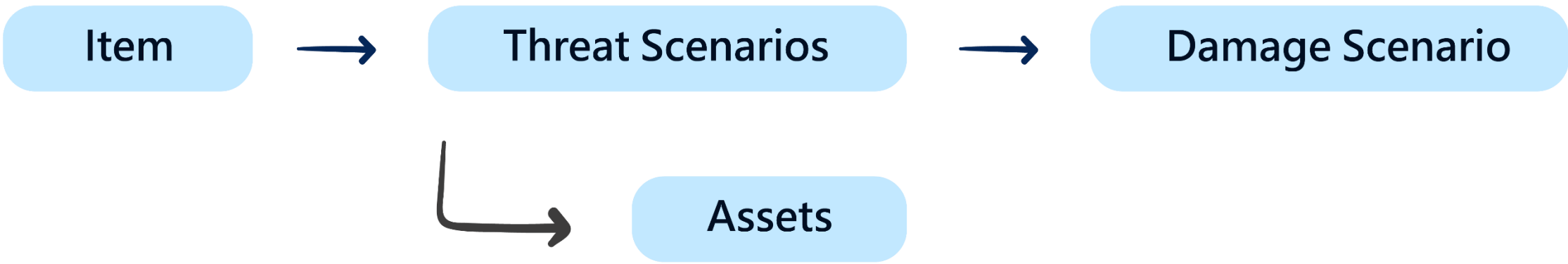
Threat Scenario	STRIDE	Asset	Damage	Impact Analysis	Attack
🔗 ISO-689 - Attacker injects spoofing system	Spoofing	🔗 ISO-684 - I/F to speech recognition system	🔗 ISO-685 - Manipulation of target data	<span style="background-color: #ffcc00; padding: 2px;">S</span> <span style="background-color: #ff0000; color: white; padding: 2px;">F</span> <span style="background-color: #ffcc00; padding: 2px;">O</span> <span style="background-color: #ff0000; color: white; padding: 2px;">P</span> <span style="background-color: #ff0000; color: white; padding: 2px;">H</span>	
🔗 ISO-689 - Attacker injects spoofing system	Spoofing	🔗 ISO-684 - I/F to speech recognition system	🔗 ISO-686 - Reading of target data	<span style="background-color: #ffcc00; padding: 2px;">S</span> <span style="background-color: #ff0000; color: white; padding: 2px;">F</span> <span style="background-color: #ffcc00; padding: 2px;">O</span> <span style="background-color: #ff0000; color: white; padding: 2px;">P</span> <span style="background-color: #ff0000; color: white; padding: 2px;">H</span>	
🔗 ISO-689 - Attacker injects spoofing system	Spoofing	🔗 ISO-682 - Wlan connection for mobile app	🔗 ISO-687 - Publishing of hijacked data when communicating with mobile devices	<span style="background-color: #ffcc00; padding: 2px;">S</span> <span style="background-color: #ff0000; color: white; padding: 2px;">F</span> <span style="background-color: #ffcc00; padding: 2px;">O</span> <span style="background-color: #ff0000; color: white; padding: 2px;">P</span> <span style="background-color: #ff0000; color: white; padding: 2px;">H</span>	

### Damage Scenarios

🚗 Manage Damage Scenarios

Asset	Damage Scenario	Security Property	Stakeholder	Impact Analysis
🔗 ISO-684 - I/F to speech recognition system	🔗 ISO-685 - Manipulation of target data	Integrity	Road User	<span style="background-color: #ffcc00; padding: 2px;">S</span> <span style="background-color: #ff0000; color: white; padding: 2px;">F</span> <span style="background-color: #ffcc00; padding: 2px;">O</span> <span style="background-color: #ff0000; color: white; padding: 2px;">P</span>
🔗 ISO-684 - I/F to speech recognition system	🔗 ISO-686 - Reading of target data	Confidentiality	Road User	<span style="background-color: #008000; padding: 2px;">S</span> <span style="background-color: #008000; color: white; padding: 2px;">F</span> <span style="background-color: #ffcc00; padding: 2px;">O</span> <span style="background-color: #ff0000; color: white; padding: 2px;">P</span>
🔗 ISO-684 - I/F to speech recognition system	🔗 ISO-14 - Unauthorized disclosure	Authenticity	Road User	<span style="background-color: #008000; padding: 2px;">S</span> <span style="background-color: #008000; color: white; padding: 2px;">F</span> <span style="background-color: #008000; color: white; padding: 2px;">O</span> <span style="background-color: #ffcc00; padding: 2px;">P</span>
🔗 ISO-682 - Wlan connection for mobile app	🔗 ISO-687 - Publishing of hijacked data when communicating with mobile devices	Confidentiality	OEM	<span style="background-color: #008000; padding: 2px;">S</span> <span style="background-color: #ff0000; color: white; padding: 2px;">F</span> <span style="background-color: #ffcc00; padding: 2px;">O</span> <span style="background-color: #ff0000; color: white; padding: 2px;">P</span>
🔗 ISO-682 - Wlan connection	🔗 ISO-688 - Hijacking of transferred data	Authenticity	OEM	<span style="background-color: #ffcc00; padding: 2px;">S</span> <span style="background-color: #008000; color: white; padding: 2px;">F</span> <span style="background-color: #008000; color: white; padding: 2px;">O</span> <span style="background-color: #ffcc00; padding: 2px;">P</span>

# Automotive cybersecurity x Polarion ALM



03

# Automotive cybersecurity x Polarion ALM

安全需求管理

# Automotive cybersecurity x Polarion ALM

**\*Title:**  
Enter Title

**\*Version:**  
Enter Version

**\*Description:**  
Enter Description

Is this Item an E/E item or component?

Does the Item contribute to the safe operation of the vehicle?

Does the Item implement functions which require collection or processing of user-related data?

Does the Item implement vehicle functions based on network components?

Is the Item to be re-used?

Is there an out-of-context component?

Is the Item an off-the-shelf component?

**Create**

使用者透過表單開啟新的Item，並根據表單選項，  
自動化判斷是否需要產生相對應  
Live Doc、WorkItem、TestPlan、Test Report

這邊我們建立一個新 Item:User Interface for GPS  
based navigation system





# Automotive cybersecurity x Polarion ALM

Created: 2022-11-24 11:25, Updated: 2024-04-10 10:45

## ISO-664 - User Interface for GPS based navigation system

ISO-680 ISO-681 ISO-682 ISO-683 ISO-684 ISO-690

Type: **Item**  
Author: **System Administrator**  
Assignee(s): **System Administrator**  
Analysis Progress:

Status: **In Analysis**  
Version: **1.0**  
Cyber Security Relevance: **yes**  
Cyber Security Plan: **01 Concept / User Interface for GPS based navigation system - 1.0 - Cybersecurity Plan**  
Cybersecurity Case: **01 Concept / User Interface for GPS based navigation system - 1.0 - Cybersecurity Case**

Out-of-Context Component:  
Off-the-Shelf Component:  
Re-Use Candidate:  
Re-Use Analysis:

### Cybersecurity Relevance Details

E/E Contribution: **yes**  
Safe Operation: **yes**  
User Related Data: **yes**  
Network Components:

### Description

UI for entering target data to navigate with the car

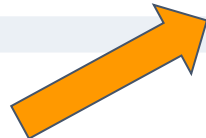
### Comments

Create Comment Collapse All Expand All View: **Tree**  Show resolved comments

### Approvals

### Linked Work Items

Suspect	Role	Title	Project	Revision	Status
	is related to	ISO-680 - Message broker	ISO21434		🟢
	is related to	ISO-681 - USB Controller	ISO21434		🟢
	is related to	ISO-682 - Wlan connection for mobile app	ISO21434		🟢
	is related to	ISO-683 - I/F for entering data on in-vehicle device	ISO21434		🟢
	is related to	ISO-684 - I/F to speech recognition system	ISO21434		🟢
	is assessed by	ISO-690 - Risk of disclosing target data	ISO21434		🟡



自動產生  
Cybersecurity Plan

## User Interface for GPS based navigation system - 1.0 - Cybersecurity Plan

### Table of Contents

- 1 Introduction
- 2 Document Information
- 3 Dependencies on other activities or information
- 4 Cybersecurity Plan Assignment:
- 5 Personnel Responsible for Performing an Activity
- 6 Required Resources for Performing an Activity
- 7 Cybersecurity Tailoring
  - 7.1 Reuse Development
  - 7.2 Component out-of-context
  - 7.3 Off-the-shelf component

### 1 Introduction

- **Project Overview**

(Provide a description of the project)

- **Cybersecurity objective**

Define the objectives, including:

- a) cybersecurity architecture.
- b) how the cybersecurity specifications will conform and be verified from higher levels of architectural abstraction;
- c) how component weaknesses will be identified; and
- d) In what way will the project provide evidence that the product conforms to the cybersecurity specifications?

- **Document References**

- **External Documents** (Provide the following information on other documents):

- Ref. No (This is a self-assigned sequential number)
- Document Title (Provide a text box)
- Revision (Provide a small text box)
- Release Date (date format)
- Author (Provide a small text box)

- **Internal Documents** (Provide the following information):

- Ref. No (This is a self-assigned, continuous sequential number from the external document ref. no.)
- Document Title (Provide a text box)
- Revision (Provide a small text box)
- Release Date (date format)
- Author (Provide a small text box)

### 2 Document Information

根據Cybersecurity Plan自動產出 Workitem，確保 Plan 中所有項目都被執行

Cybersecurity Plan 自動產出的內容與工作項目皆可透過 Polarion ALM 製作成 Template。以確保所有驗證過程中符合ISO 標準/公司規範。

# Automotive cybersecurity x Polarion ALM

Created: 2022-11-24 11:25, Updated: 2024-04-10 10:45

## 自動產生相對應 WorkItem

ISO-665 +  
ISO-672 - Cybersecurity Tailoring  
ISO-673 ISO-674 ISO-675 +

Type: **Heading**  
Severity: **Normal**  
Author: **System Administrator**  
Project: **ISO21434**  
Categories:

Initial Estimate:  
Time Spent:  
Remaining Estimate:

Assignee(s):  
Status: **Open**  
Resolution:

Priority: **Medium [50.0]**  
Due Date:  
Time Point:  
Planning Constraints:  
Planned To:

**Description**

**Comments**  
Create Comment Collapse All Expand All View: **Tree**  Show resolved comments

**Work Records**

**Approvals**

**Linked Revisions**

**Linked Work Items**

Suspect	Role	Title	Project	Revision	Status	Assignee(s)
	relates to	ISO-665 - User Interface for GPS based navigation system - 1.0 - Cybersecurity Plan	ISO21434		Open	
	is related to	ISO-673 - Reuse Development	ISO21434		Open	
	is related to	ISO-674 - Component out-of-context	ISO21434		Open	
	is related to	ISO-675 - Off-the-shelf component	ISO21434		Open	

# Automotive cybersecurity x Polarion ALM

Created: 2022-11-24 11:25, Updated: 2024-04-10 10:45

## ISO-664 - User Interface for GPS based navigation system

ISO-680 ISO-681 ISO-682 ISO-683 ISO-684 ISO-690

Type: **Item**  
Author: **System Administrator**  
Assignee(s): **System Administrator**  
Analysis Progress:

Status: **In Analysis**  
Version: **1.0**  
Cyber Security Relevance: **yes**  
Cyber Security Plan: **01 Concept / User Interface for GPS based navigation system - 1.0 - Cybersecurity Plan**  
Cybersecurity Case: **01 Concept / User Interface for GPS based navigation system - 1.0 - Cybersecurity Case**

Out-of-Context Component:  
Off-the-Shelf Component:  
Re-Use Candidate:  
Re-Use Analysis:

### Cybersecurity Relevance Details

E/E Contribution: **yes**  
Safe Operation: **yes**  
User Related Data: **yes**  
Network Components:

### Description

UI for entering target data to navigate with the car

### Comments

Create Comment Collapse All Expand All View: **Tree**  Show resolved comments

### Approvals

### Linked Work Items

Suspect	Role	Title	Project	Revision	Status
	is related to	ISO-680 - Message broker	ISO21434		🟢
	is related to	ISO-681 - USB Controller	ISO21434		🟢
	is related to	ISO-682 - WLAN connection for mobile app	ISO21434		🟢
	is related to	ISO-683 - I/F for entering data on in-vehicle device	ISO21434		🟢
	is related to	ISO-684 - I/F to speech recognition system	ISO21434		🟢
	is assessed by	ISO-690 - Risk of disclosing target data	ISO21434		🟡

自動產生 Work Item



04

# Automotive cybersecurity x Polarion ALM

風險管理與漏洞追蹤



## Item Overview

- New Item
- Damage Scenarios Library
- Threat Scenarios Library

### Active Cybersecurity Items

Item	Status	Assignee(s)	Actions			
ISO-664 - User Interface for GPS ba...	In Analysis	System Administrator	<a href="#">View</a>	<a href="#">Assets &amp; Damages</a>	<a href="#">Threat Scenarios</a>	<a href="#">Attack Path &amp; Risks</a>
ISO-692 - User Interface for GPS ba...	Open		<a href="#">View</a>	<a href="#">Assets &amp; Damages</a>	<a href="#">Threat Scenarios</a>	<a href="#">Attack Path &amp; Risks</a>

Active Cybersecurity Items contain objects in status *Open* and *In Analysis*

### Closed Cybersecurity Items

Closed Cybersecurity Items contain objects in status *Analysed* and *Retired*

點擊 Threat Scenarios 可進入總覽畫面





## TARA - Threat Scenarios

- Item View
- Damage Scenarios
- Attack Paths & Risks
- User Guide

Selected Item : ISO-664 - User Interface for GPS based navigation system  
 Assignee : System Administrator  
 Status : In Analysis

- Create New Threat
- Add From Library

### Threat Scenario

ISO-689 - Attacker injects spoofing system

Threat 底下可以連接  
相對應受影響項目



### Stride Selector

Spoofting

### Impact Analysis

S F O P

Damage Scenario	Affected Asset	Stakeholder	Impact Analysis
ISO-685 - Manipulation of target data	ISO-684 - I/F to speech recognition system	Road User	S F O P
ISO-686 - Reading of target data	ISO-684 - I/F to speech recognition system	Road User	S F O P
ISO-687 - Publishing of highjacked data when communicating with mobile devices	ISO-682 - Wlan connection for mobile app	OEM	S F O P



## Item Overview

- [New Item](#)
- [Damage Scenarios Library](#)
- [Threat Scenarios Library](#)

### Active Cybersecurity Items

Item	Status	Assignee(s)	Actions			
<a href="#">ISO-664 - User Interface for GPS ba...</a>	In Analysis	System Administrator	<a href="#">View</a>	<a href="#">Assets &amp; Damages</a>	<a href="#">Threat Scenarios</a>	<a href="#">Attack Path &amp; Risks</a>
<a href="#">ISO-692 - User Interface for GPS ba...</a>	Open		<a href="#">View</a>	<a href="#">Assets &amp; Damages</a>	<a href="#">Threat Scenarios</a>	<a href="#">Attack Path &amp; Risks</a>

Active Cybersecurity Items contain objects in status **Open** and **In Analysis**

### Closed Cybersecurity Items

Closed Cybersecurity Items contain objects in status **Analysed** and **Retired**



接著可以進入 **Attack Path and Risks** 畫面





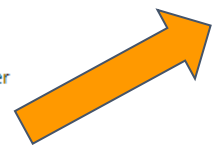


## TARA - Attack Path and Risks

- [Item View](#)
- [Damage Scenarios](#)
- [Threat Scenarios](#)
- [User Guide](#)

**Selected Item :** ISO-664 - User Interface for GPS based navigation system  
**Assignee :** System Administrator  
**Status :** In Analysis

Threat Scenario	Stride	Impact Rating	Attack Feasibility	Risk Treatment																																																															
ISO-689 - Attacker injects spoofing system	Spoofing	S F O P	[Red Box]	ISO-690 - Risk of disclosing target data																																																															
<table border="1"> <thead> <tr> <th>Attack Path</th> <th>Elapsed Time</th> <th>Expertise</th> <th>Knowledge</th> <th>Window of Opportunity</th> <th>Equipment</th> <th>Attack Feasibility</th> </tr> </thead> <tbody> <tr> <td>Main Path</td> <td>&lt;= 1 day</td> <td>Layman</td> <td>Public Information</td> <td>Unlimited</td> <td>Standard</td> <td>High</td> </tr> <tr> <td colspan="2"><b>Attack Step</b></td> <td colspan="4"><b>Affected Asset</b></td> </tr> <tr> <td colspan="2">Attack via usb controller</td> <td colspan="4">ISO-681 - USB Controller</td> </tr> <tr> <td colspan="2">Sending overflow message to enter maintenance mode</td> <td colspan="4">ISO-680 - Message broker</td> </tr> <tr> <td>Wireless Attack Path</td> <td>&gt; 6 months</td> <td>Multiple Experts</td> <td>Strictly Confidential Information</td> <td>Difficult</td> <td>MultipleBespoke</td> <td>Very Low</td> </tr> <tr> <td colspan="2"><b>Attack Step</b></td> <td colspan="4"><b>Affected Asset</b></td> </tr> <tr> <td colspan="2">Manipulation of Wireless device (outside our assets)</td> <td colspan="4">ISO-682 - Wlan connection for mobile app</td> </tr> <tr> <td colspan="2">Transferring manipulated connect strings via Wlan access controller/Fifo</td> <td colspan="4">ISO-682 - Wlan connection for mobile app</td> </tr> <tr> <td colspan="2">Adjusting dynamically offset messages</td> <td colspan="4">ISO-680 - Message broker</td> </tr> </tbody> </table>					Attack Path	Elapsed Time	Expertise	Knowledge	Window of Opportunity	Equipment	Attack Feasibility	Main Path	<= 1 day	Layman	Public Information	Unlimited	Standard	High	<b>Attack Step</b>		<b>Affected Asset</b>				Attack via usb controller		ISO-681 - USB Controller				Sending overflow message to enter maintenance mode		ISO-680 - Message broker				Wireless Attack Path	> 6 months	Multiple Experts	Strictly Confidential Information	Difficult	MultipleBespoke	Very Low	<b>Attack Step</b>		<b>Affected Asset</b>				Manipulation of Wireless device (outside our assets)		ISO-682 - Wlan connection for mobile app				Transferring manipulated connect strings via Wlan access controller/Fifo		ISO-682 - Wlan connection for mobile app				Adjusting dynamically offset messages		ISO-680 - Message broker			
Attack Path	Elapsed Time	Expertise	Knowledge	Window of Opportunity	Equipment	Attack Feasibility																																																													
Main Path	<= 1 day	Layman	Public Information	Unlimited	Standard	High																																																													
<b>Attack Step</b>		<b>Affected Asset</b>																																																																	
Attack via usb controller		ISO-681 - USB Controller																																																																	
Sending overflow message to enter maintenance mode		ISO-680 - Message broker																																																																	
Wireless Attack Path	> 6 months	Multiple Experts	Strictly Confidential Information	Difficult	MultipleBespoke	Very Low																																																													
<b>Attack Step</b>		<b>Affected Asset</b>																																																																	
Manipulation of Wireless device (outside our assets)		ISO-682 - Wlan connection for mobile app																																																																	
Transferring manipulated connect strings via Wlan access controller/Fifo		ISO-682 - Wlan connection for mobile app																																																																	
Adjusting dynamically offset messages		ISO-680 - Message broker																																																																	





# 風險管理與漏洞追蹤

## IARA - Attack Path and Risks

- Item View
- Damage Scenarios
- Threat Scenarios
- User Guide

Selected Item : ISO-664 - User Interface for GPS based navigation system  
 Assignee : System Administrator  
 Status : In Analysis

Threat Scenario		Stride	Impact Rating	Attack Feasibility	Risk Treatment	
ISO-689 -				ISO-690 - Risk		
		Attack Feasibility				
		Attack Feasibility				
		Attack Feasibility				
		Attack Feasibility				
S F O P	Impact		Very Low	Low	Medium	High
		Severe	2	3	4	5
		Major	2	3	3	4
		Moderate	2	2	2	3
	Negligible	1	1	1	2	

ISO-690 - Risk of disclosing target data

Fields

Assignee(s): --

\*Status: Draft

Risk Safety: Very High (5)

Risk Finance: Very High (5)

Risk Operation: Very High (5)

Risk Privacy: Very High (5)

Risk Treatment: Retaining the risk

Polarion 也根據影響值設定風險嚴重性等級



05

# Automotive cybersecurity x Polarion ALM

監控和持續改進



## Item Overview

- New Item
- Damage Scenarios Library
- Threat Scenarios Library

### Active Cybersecurity Items

Item	Status	Assignee(s)	Actions			
ISO-664 - User Interface for GPS ba...	In Analysis	System Administrator	<a href="#">View</a>	<a href="#">Assets &amp; Damages</a>	<a href="#">Threat Scenarios</a>	<a href="#">Attack Path &amp; Risks</a>
ISO-692 - User Interface for GPS ba...	Open		<a href="#">View</a>	<a href="#">Assets &amp; Damages</a>	<a href="#">Threat Scenarios</a>	<a href="#">Attack Path &amp; Risks</a>

Active Cybersecurity Items contain objects in status *Open* and *In Analysis*

### Closed Cybersecurity Items

Closed Cybersecurity Items contain objects in status *Analysed* and *Retired*

最後我們來看監控儀表板與報表





# 監控和持續改進

## Item View

Item: ISO-664 - User Interface for GPS based navigation system Item responsible: System Administrator  
Status: In Analysis [Select Another Item](#)

### Document Overview

Document	Status	Type	Author
User Interface for GPS based navigation system - 1.0 - Cybersecurity Plan	Draft	Cybersecurity Plan	System Administrator
User Interface for GPS based navigation system - 1.0 - Cybersecurity Case	Draft	Cybersecurity Case	System Administrator

### Asset Overview

[Manage Assets](#)

Asset

- ISO-683 - I/F for entering data on in-vehicle device  Open
- ISO-684 - I/F to speech recognition system  Open
- ISO-681 - USB Controller  Open
- ISO-682 - Wlan connection for mobile app  Open
- ISO-680 - Message broker  Open

使用者建立的所有 Document、Risk、Threat 都可以在儀表板上進行監控

### Risks

[Manage Attack Paths & Risks](#)

Risk	Status	Assignee	Risk Severity	Risk Treatment	Goal/Claim
ISO-690 - Risk of disclosing target data	Draft			Retaining the risk	

### Threat Scenarios

[Manage Threat Scenarios](#)

Threat Scenario	STRIDE	Asset	Damage	Impact Analysis	Attack
ISO-689 - Attacker injects spoofing system	Spoofing	ISO-684 - I/F to speech recognition system	ISO-685 - Manipulation of target data		
ISO-689 - Attacker injects spoofing system	Spoofing	ISO-684 - I/F to speech recognition system	ISO-686 - Reading of target data		
ISO-689 - Attacker injects spoofing system	Spoofing	ISO-682 - Wlan connection for mobile app	ISO-687 - Publishing of highjacked data when communicating with mobile devices		
ISO-704 - Attacker injects spoofing system	-	-	-		

### Damage Scenarios

[Manage Damage Scenarios](#)

Asset	Damage Scenario	Security Property	Stakeholder	Impact Analysis
ISO-684 - I/F to speech recognition system	ISO-685 - Manipulation of target data	Integrity	Road User	
ISO-684 - I/F to speech recognition system	ISO-686 - Reading of target data	Confidentiality	Road User	
ISO-684 - I/F to speech recognition system	ISO-14 - Unauthorized disclosure	Authenticity	Road User	
ISO-682 - Wlan connection for mobile app	ISO-687 - Publishing of highjacked data when communicating with mobile devices	Confidentiality	OEM	
ISO-682 - Wlan connection for mobile app	ISO-688 - Highjacking of transferred data when communicating with mobile devices	Authenticity	OEM	





06

# Polarion X

SaaS ALM solution

## Polarion Test Drives

Take Polarion for a spin for free today and get a feel for the tool that helps more than 20,000 firms worldwide create better complex software faster.



### Polarion ALM

Everything you need to manage your development process. Connect your development process to requirements, coding, testing, and release.

[Launch](#)

### Polarion X

Software Lifecycle Under Control in the Cloud. Everything you need to achieve agility and have full control over your cyber-physical systems application lifecycle.

[Launch](#)

想要立刻體驗 Polarion 嗎，趕快使用 PolarionX(SaaS ALM solution)



## Create New Project ✕

**豐富的專案範本輕鬆上手 Polarion**

Following Steps:

- Basics
- Template**
- Summary
- Creation

V-Model Project (Concept, Requirements, Design, Risks, Planning, Development, Testing, Maintenance) ▾

-- no template (empty project) --

- Agile Software Project (Product and Release Backlogs, Sprint Management, Quality Assurance, Builds)
- Drive Pilot (Demo based on V-Model Project)
- Drive Pilot QA (Demo based on V-Model Project)
- Drive Pilot REQ (Demo based on V-Model Project)
- E-Library (Demo based on Agile Software Project)
- ISO21434 Cybersecurity, build: 20230323-1955
- ISO26262 Functional Safety (FuSa), build: 20230329-2012
- Lane Fusion Example FuSa (Demo based on ISO26262 Functional Safety (FuSa)), build: 20230329-2012
- Nextedy GANTT Demo**
- Nextedy PLANNINGBOARD Demo
- Specification Project with Teamcenter Variant Management (Requirements, Testing)
- Specification Project with Variant Management (Requirements, Testing, Variants, Features)
- User Interface Cybersecurity (Demo based on ISO21434 Cybersecurity), build: 20230323-1955
- V-Model Project (Concept, Requirements, Design, Risks, Planning, Development, Testing, Maintenance, Builds)
- V-Model Project QA (Concept, Requirements, Design, Risks, Development, Testing, Maintenance, Builds)**
- V-Model Project REQ (Concept, Requirements, Design, Risks, Maintenance)
- Weather Station (Demo project based on Specification Project with Variant Management)

[Previous](#) [Next](#)



46afdfb5428b4edab9e6  
3559b903b3471

Default Space ▶ User Guide

Default work item workflow  
Hazardous Event Workflow  
Test Case Workflow

Expand Tools

家丞 (Jason) 薛  
My Polarion

- 03 Functional Safety Concept
- 04 Technical Safety Concept
- 05 Safety Validation

Documents & Pages

- Default Space
  - Index
  - Administration Guide
  - User Guide
- Document Templates
- Functional Safety - Documents
- Functional Safety - Reports
- How To
- Testing - Documents
- Testing - Reports
  - Index
  - REQ\_FSC\_FSC\_TestCases
  - REQ\_HSR\_HSR\_TestCase
  - REQ\_SSR\_SSR\_TestCases
  - REQ\_TSR\_TSR\_TestCases
  - Safety Validation - Information
  - Test Cases
  - Test Cases by Type Overview

### Introduction

This Polarion template and workflow are designed to support the development, verification, validation, and the traceability between these important functional safety activities. The use of libraries and templates helps to standardize the process and reduce the risk of errors.

### Data Model

This is the template's Data Model. Standard Polarion links connect all elements.

```
graph TD
    IS[Item System] --- C[Component]
    C --- F[Functionality]
    F --- FM1[Failure Mode]
    F --- FM2[Failure Mode]
    F --- FM3[Failure Mode]
    F --- FM4[Failure Mode]
    FM1 --- Risk[Risk]
    FM2 --- Risk
    FM3 --- Risk
    FM4 --- Risk
    Risk --- IRA[Initial Risk Assessment]
    Risk --- Hazards[Hazards]
    IRA --- RA[Recommended Actions]
    RA --- RRA[Residual Risk Assessment]
    Hazards --- HE[Hazardous Event]
    HE --- SG[Safety Goal]
    SG --- SS[Safe State]
    SS --- Fi1[Failure]
    SS --- Fi2[Failure]
    SG --- SV[Safety Validation]
```

**Initial Risk Assessment**

- Accepted
- ALARP
- NOT Accepted

**Residual Risk Assessment**

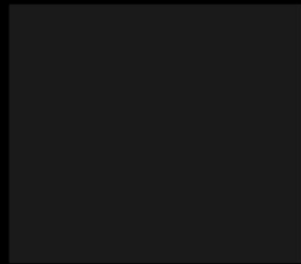
- Accepted
- ALARP
- NOT Accepted

Severity: S3  
Controllability: C1  
Exposure: E4  
ASIL Classification: ASIL B

每個範本中都有相對應的使用者手冊  
輕鬆上手想要試用的專案範本!!!



Q&A



聯絡資訊

## Contact Information

Harry Lu 盧致均

Email : harry@devops.com.tw

Moblie : (02)7752-7696 #160

Jason Xue 薛家丞

Email : Jason@devops.com.tw

Moblie : (02)7752-7696 #163

Jos Hsu 許智閔

Email : jos@devops.com.tw

Moblie : (02)7752-7696 #168

THANK YOU



DevOps Tec.

戴博斯科技股份有限公司



Facebook



官網