Regular Paper

Communications of the CCISA
Vol. 31 No. 4 Nov. 2025

基於 Zeek 與 SAGE 的工控系統自動化攻擊圖建構方法

林子婷[1]、王紹睿[2*]
[1,2]國立臺灣科技大學資訊工程系
[1]M11311001@mail.ntust.edu.tw、[2]shaojuiwang@mail.ntust.edu.tw

摘要

本研究針對工控系統在面對日益複雜的資安威脅下所面臨的三大挑戰: 事件資料碎片化、跨域攻擊鏈難以重建、以及攻擊圖缺乏可解釋性與標準化，提出一套基於 Zeek 與 SAGE 的自動化攻擊圖建構系統。系統核心目標在於：將 Zeek 所產生的工控網路日誌轉換為具語意的事件序列、利用非監督式的 S-PDFA 演算法自動建構攻擊行為模型，並結合 MITRE ATT&CK for ICS 框架生成具標準化與視覺化的攻擊圖。本研究設計四階段事件抽象化流程，實現協定層行為的結構化轉換；同時導入目標導向的攻擊圖建構策略，提升對多階段、低頻攻擊行為的識別能力。實驗採用自建之標準化 Modbus 攻擊資料集與公開 SCADA HMI 攻擊資料集進行驗證。結果顯示，本系統能以 6 分鐘完成七類攻擊行為分析，達成最高 764:1 的事件壓縮比，並成功處理包含 117 萬筆封包的真實攻擊資料。生成之攻擊圖具高度可解釋性與技術分類對應性，支援 15 類主要攻擊類型與 83 個 ATT&CK 技術標準。本研究成果有效緩解 OT 環境中的告警疲勞與關鍵威脅遺漏問題，並提供一個具可行性、可擴充性與標準化潛力的工控威脅建模解決方案。

關鍵詞：工業控制系統、攻擊圖、Zeek、SAGE、S-PDFA、MITRE ATT&CK for ICS

* 通訊作者 (Corresponding author.)

Communications of the CCISA
Vol. 31 No. 4 Nov. 2025

Automated Attack Graph Construction for Industrial Control Systems Based on Zeek and SAGE

Tzu-Ting Lin[1], Peter Shaojui Wang[2*]
[1,2]Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology
[1]M11311001@mail.ntust.edu.tw, [2]shaojuiwang@mail.ntust.edu.tw

Abstract

This study tackles three key cybersecurity challenges in Industrial Control Systems (ICS): fragmented event data, difficulty reconstructing cross-domain attack chains, and low explainability and standardization in attack graphs. To address these issues, we propose an automated attack graph construction system combining Zeek for ICS traffic analysis and SAGE for behavior modeling via an unsupervised S-PDFA algorithm. The system transforms Zeek logs into semantic event sequences, builds behavior models, and generates visual, standardized graphs aligned with the MITRE ATT&CK for ICS framework. We implement a four-stage event abstraction pipeline for structured protocol-aware transformation, and adopt a goal-oriented attack graph strategy to better detect multi-stage, low-frequency threats. Experiments on a custom Modbus dataset and a public SCADA HMI dataset confirm the system's effectiveness: analyzing seven attack types in under 6 minutes, achieving a 764:1 compression ratio, and processing over 1.17 million packets. The resulting graphs demonstrate strong explainability and coverage of 15 attack categories and 83 ATT&CK techniques.

Keywords: Industrial Control Systems (ICS), Attack Graph, Zeek, SAGE, S-PDFA, MITRE ATT&CK for ICS

壹、前言

隨著工業 4.0 與數位化轉型的推進，工業控制系統 (Industrial Control Systems, ICS) 網路安全已成為關鍵基礎設施保護的核心議題。過去多採實體隔離的營運技術 (Operational Technology, OT) 網段，正逐步與資訊技術 (Information Technology, IT) 環境深度整合，這種 IT/OT 融合在提升營運效率的同時，也為惡意攻擊者開啟前所未有的入侵管道 [1] [2]。在多階段入侵與告警過載情境下，現有分析工具往往無法即時重建攻擊鏈，導致 OT 威脅偵測與行為關聯分析效能受限。

目前工控環境面臨的威脅呈現出前所未有的複雜性。研究顯示，在多數 OT 入侵事件中，製造業已成為最受攻擊的產業，在勒索軟體和資料洩漏攻擊中首當其衝 [1]。這些攻擊不僅影響傳統的 IT 系統，更直接威脅到控制實體製程的 OT 設備，包括監控與資料擷取系統 (SCADA)、可程式邏輯控制器 (PLC) 以及分散式控制系統 (DCS) 等關鍵元件[1] [2]。

為因應這些挑戰，本研究提出一套基於 Zeek 與 SAGE 的自動化攻擊圖建構系統。系統核心目標在於：將 Zeek 所產生的工控網路日誌轉換為具語意的事件序列、利用非監督式的 S-PDFA 演算法自動建構攻擊行為模型，並結合 MITRE ATT&CK for ICS 框架生成具標準化與視覺化的攻擊圖。

貳、文獻探討

2.1 攻擊圖技術與工控環境應用現況

攻擊圖 (Attack Graph) 是一種用於描述攻擊者如何利用系統漏洞實現攻擊目標的圖形化表示方法。Phillips 與 Swiler 於 1998 年首次提出攻擊圖概念 [3]，隨後 Ou 等人於 2006 年提出可擴展性攻擊圖生成方法 [4]。然而，傳統攻擊圖生成方法多採用拓撲漏洞分析途徑，高度依賴預先定義的網路拓撲資訊與公開漏洞資料庫。工控環境具有高度封閉性，且廣泛使用專有協定與客製化系統，導致公開漏洞資訊嚴重不足 [5]。

2.2 MITRE ATT&CK for ICS 框架

美國非營利研究機構 MITRE 於 2020 年推出針對工業控制系統的對抗戰術、技術和通用知識框架 (MITRE ATT&CK for ICS) [6]。根據 2025 年最新版本 (v17)，該框架共定義 12 項戰術，從初始存取到最終影響，共計 83 個 ICS 特定技術 [7]。與企業版 MITRE ATT&CK for Enterprise 不同，ICS 版本特別強調對物理過程的影響，包括安全性損失、可用性損失、以及生產力和收入損失等直接關係到工業運作的技術 [6]。

2.3 Zeek 與 SAGE 技術

Zeek 是一款混合式入侵偵測系統，結合特徵式與異常式技術。其分析引擎會將收集到的網路封包轉換為一系列事件，以支援上下文導向且具彈性的資安策略撰寫 [8]。為強化對工控協定的支援，Zeek 社群與美國愛達荷國家實驗室共同維護的 ICSNPP 套件提供 16 種完整的協定解析器 [9]。SAGE (IntruSion alert-driven Attack Graph Extractor) 系統由 Nadeem 等人於 2021 年提出[10] [11]，採用 S-PDFA 演算法建模警示之間的時間與機率依賴關係。相較於頻率導向的方法，SAGE 將「不頻繁但高嚴重性」的警示視為建模重點，其後綴導向的設計可將稀有攻擊行為置於學習模型的核心 [11]。

參、研究方法

3.1 系統整體架構

本研究提出的系統採用三層式架構設計，確保模組間的低耦合與高內聚。整體架構分為資料來源層、行為建模層與攻擊圖生成層，各層透過明確定義的介面進行資料交換。這種分層設計不僅提升系統的模組化程度，更使得各層可以獨立優化和升級。

資料來源層負責網路流量的即時解析與結構化日誌生成，是整個系統的資料入口。核心元件為 Zeek 網路安全監控框架，其採用事件驅動架構，將網路封包轉換為高階協定事件。Zeek 的設計理念著重於協定語意理解而非單純的特徵比對，這種深度封包檢測能力使其能夠解析應用層協定內容並提供豐富的上下文資訊。對於工控環境，本研究整合 ICSNPP 協定解析器套件，主要使用 ICSNPP-Modbus 模組進行 Modbus 協定的深度解析。

行為建模層包含欄位萃取模組、事件編碼引擎與 S-PDFA 學習器。欄位萃取模組負責從結構化日誌中提取關鍵資訊，對於 modbus.log 重點萃取時間戳記、來源與目的 IP、功能碼、暫存器地址、數值等欄位。事件編碼引擎實作三層編碼策略：協定層編碼將原始功能碼關聯至操作類別；行為層編碼結合時序與頻率特徵識別異常模式；攻擊層編碼將識別出的行為對應至 MITRE ATT&CK for ICS 技術分類。

攻擊圖生成層負責從 S-PDFA 模型產生可視化的攻擊圖，是系統的輸出介面。該層包含目標事件識別模組、路徑回溯模組與視覺化引擎。目標事件識別模組首先掃描所有事件序列，識別嚴重度超過預設閾值的目標事件，如參數修改 (MODIFY_PARAMETERS，嚴重度 100)、未授權命令 (UNAUTHORIZED_COMMAND_MESSAGE，嚴重度 100)、服務阻斷 (DENIAL_OF_SERVICE_ICS，嚴重度 90) 等。

3.2 Zeek 日誌結構與內容

Zeek 產生的日誌具有高度結構化特性，採用 Tab 分隔值 (TSV) 格式儲存，便於程式化處理。每個日誌檔案包含檔頭元資料和資料內容兩部分，檔頭定義欄位名稱、資料類型、時間戳記格式等元資訊，確保日誌的自描述性。

以 Modbus 協定為例，modbus.log 的典型記錄包含以下關鍵欄位：時間戳記 (ts) 記錄精確到微秒的事件時間；連線識別碼 (uid) 用於關聯相關的網路活動；來源與目的網路位址 (id.orig_h、id.resp_h) 及埠號；Modbus 特定欄位如功能碼 (func)、交易識別碼 (tid)、單元識別碼 (unit)、起始地址 (start_address)、數量 (quantity)、數值 (values) 等。conn.log 提供連線層面的統計視圖，包含每個連線的持續時間、傳輸位元組數、封包數、連線狀態等彙總資訊。notice.log 記錄 Zeek 腳本產生的告警事件，每條記錄包含告警類型、訊息、相關連線等資訊。

3.3 四階段事件抽象化流程

本研究設計四階段的事件抽象化流程，系統化地將原始日誌轉換為語意豐富的事件序列。第一階段為資料選擇，根據分析目標選擇相關的日誌類型。系統預設選擇 modbus.log、conn.log、notice.log 作為主要資料來源，這些日誌包含工控攻擊分析所需的核心資訊。

第二階段為欄位擷取，針對不同日誌類型擷取具代表性的欄位。對於 modbus.log 重點擷取功能碼、地址、數值等直接反映操作意圖的欄位；對於 conn.log 關注連線時長、資料量等可能指示異常的統計特徵。第三階段為事件編碼，將擷取的欄位資訊根據預定義規則轉換為標準化的事件代碼。例如連續的讀取操作若針對同一地址範圍且頻率異常，編碼為 RECONNAISSANCE 事件；對關鍵暫存器的寫入操作編碼為 CRITICAL_WRITE 事件。第四階段為序列切分，將離散事件組織為具有上下文關聯的序列，系統實施雙重切分策略：基於連線的切分利用 Zeek 的 uid 欄位聚合同一連線的事件；基於時間窗的切分使用 150 秒的滑動窗口捕捉跨連線但時間相近的相關活動。

3.4 S-PDFA 模型學習過程

SAGE 採用 S-PDFA (Suffix-based Probabilistic Deterministic Finite Automaton)作為核心學習模型，其設計特別適合捕捉攻擊行為的序列特性。與傳統的前綴樹或馬可夫模型相比，S-PDFA 的核心優勢在於對低頻高危事件的敏感性。透過學習基於後綴的模型，系統能夠識別那些出現頻率低但會導致嚴重後果的攻擊序列。

學習過程分為四個主要步驟：第一步是前綴樹建構，將所有事件序列插入到一個共享的前綴樹結構中，樹的每個節點代表一個事件，邊代表事件間的時序關係。第二步是後綴識別與優先級標記，系統掃描前綴樹識別所有到達高嚴重度事件的路徑，這些路徑的後綴部分被賦予更高的重要性權重。第三步是狀態合併，使用 FlexFringe 實作的

ALERGIA 演算法執行，基於統計相似性度量識別具有相似後續行為的狀態並將其合併，系統設定合併閾值為 0.05、最小支援度為 3、狀態數上限為 5。第四步是機率估計與模型精煉，基於訓練資料計算每個狀態轉移的機率，使用拉普拉斯平滑處理零機率問題。

3.5 目標導向攻擊圖建構

SAGE 採用目標導向的方式建構攻擊圖，這種設計理念源於對實際安全分析需求的深入理解。安全分析師最關心的往往是那些造成實質影響的事件，以及攻擊者如何達到這些目標。系統維護一個攻擊目標分類體系，涵蓋工控環境中的主要威脅類型：資料竊取類目標包括 THEFT_OF_OPERATIONAL_INFORMATION (嚴重度 80)；服務中斷類目標包括 DENIAL_OF_SERVICE_ICS (嚴重度 90)、LOSS_OF_VIEW (嚴重度 85)；過程操控類目標包括 MODIFY_PARAMETERS (嚴重度 100)、MANIPULATION_OF_CONTROL (嚴重度 100)；安全影響類目標包括 LOSS_OF_SAFETY (嚴重度 100)。

對於每個識別出的目標事件，系統執行路徑回溯演算法。演算法從 S-PDFA 模型中的目標狀態開始，使用深度優先搜尋策略探索所有可能的前驅路徑。系統實施多項優化策略：機率閾值剪枝忽略轉移機率低於 0.01 的路徑；深度限制將搜尋深度限制在合理範圍內；相似路徑合併將只在細節上有差異的路徑聚合展示。最終生成的攻擊圖是一個有向無環圖 (DAG)，清晰展示從初始訪問到最終影響的完整攻擊鏈。

3.6 視覺化設計與輸出

攻擊圖的視覺化採用分層布局演算法，將攻擊序列的時序關係轉換為空間上的層次結構。系統運用顏色作為主要的視覺編碼通道，根據事件嚴重度關聯至綠色 (低風險，嚴重度<25)、黃色 (中風險，嚴重度 25-75)、紅色 (高風險，嚴重度>75) 的漸進色階。節點間的有向邊表示事件轉移關係，透過線條樣式區分轉移機率的高低，實線表示高機率轉移 (>0.7)，虛線表示低機率轉移，並標註時間間隔資訊。系統採用 Graphviz 圖形視覺化引擎，輸出格式包括 DOT 格式、PNG 格式與 SVG 格式，平衡可攜性、品質和後續處理的彈性需求。

肆、實驗結果

4.1 實驗設計與環境配置

本研究設計兩個互補的實驗以全面驗證系統效能。實驗設計基於三個核心假設：首先，工控系統攻擊具有明確的階段性特徵，可透過事件序列學習捕捉；其次，不同類型的攻擊展現可區分的行為模式，能夠自動分類與識別；第三，視覺化的攻擊圖能有效輔

助人類分析師理解複雜的攻擊脈絡。

實驗環境建置採用配備 Intel Core i7-1370P 處理器與 64GB 記憶體的實體主機，透過 VMware Workstation 17 Pro 建立虛擬化平台，為實驗虛擬機配置 2 個虛擬處理器核心與 16GB 記憶體。作業系統選用 Ubuntu 22.04 LTS 版本，軟體工具配置包括 Zeek 6.0.9 作為網路流量解析引擎並整合 ICSNPP-Modbus 外掛模組、Python 3.10 作為主要的程式開發環境、FlexFringe 框架實作 S-PDFA 演算法、以及 Graphviz 2.50 進行攻擊圖的視覺化呈現。

4.2 資料集特徵與選擇理由

本研究採用兩組互補性資料集進行實驗驗證。第一組為自建之 Modbus 攻擊資料集，於配備完整實體設備的工控測試環境中擷取，共計 78,436 筆 Modbus 通訊封包，涵蓋七種攻擊場景：基線重播攻擊 (467 封包)、虛假注入攻擊 (374 封包)、修改長度參數攻擊 (381 封包)、查詢洪水攻擊 (75,678 封包)、偵察攻擊 (673 封包)、堆疊 Modbus 幀攻擊 (368 封包)、寫入所有線圈攻擊 (495 封包)。

第二組採用 2023 年公開釋出的 SCADA HMI 攻擊資料集 [12]，源自實際遭受攻擊的水處理設施，包含 1,172,759 筆通訊紀錄，時間跨度達 8.3 小時，檔案大小為 100MB。攻擊活動由 IP 位址 185.175.0.3 發起，目標涵蓋 SCADA 主站、HMI 工作站、PLC 控制器及其他網路服務節點。兩組資料集的選用充分考量實驗需求的不同面向：自建資料集提供標準化、可控制的測試環境；公開資料集則反映真實攻擊的複雜性與多樣性。

4.3 實驗一：Modbus 標準攻擊分析結果

系統成功識別所有七種攻擊類型，並產生總計 72 張攻擊圖。整體執行耗時 6 分 4 秒，處理效率展現顯著差異：一般攻擊類型在 2-4 秒內完成處理，而查詢洪水攻擊因資料量龐大需要 5 分 40 秒。基線重播攻擊產生最多的攻擊圖 (53 張)，涉及超過 20 個不同的目標 IP，每個攻擊圖展示不同的技術組合，包括 MODIFY_PARAMETERS (T0836)、DENIAL_OF_SERVICE (T0814)、UNAUTHORIZED_COMMAND_MESSAGE (T0855) 等。查詢洪水攻擊雖然只產生 5 張攻擊圖，但生成最多的日誌記錄 (98,200 筆)，壓縮比達到驚人的 19,640:1。表一彙整各攻擊類型的效能指標。

表一：攻擊類型效能分析表 (Table 1: Attack Type Performance Analysis)

攻擊類型	封包數量	Zeek 解析時間	攻擊圖產生時間	攻擊圖張數	總花費時間
Baseline Replay	467	1 秒	13 秒	53	14 秒
False Injection	374	1 秒	4 秒	4	5 秒
Modify Length	381	1 秒	6 秒	3	7 秒
Query Flooding	75,678	5 分 17 秒	9 秒	5	5 分 26 秒
Reconnaissance	673	< 1 秒	4 秒	1	4 秒
Stack Frames	368	< 1 秒	4 秒	4	4 秒
Write All Coils	495	1 秒	4 秒	2	5 秒
總計	**78,436**	-	-	**72**	**6 分 5 秒**

4.4 資料壓縮比分析

壓縮比是 SAGE 系統的核心優勢之一，反映系統將大量原始數據精煉為簡潔攻擊圖的能力。實驗結果顯示，不同攻擊類型的壓縮比差異巨大，從 9:1 到 19,640:1 不等，這種差異源於攻擊行為的本質特徵。查詢洪水攻擊達到最高壓縮比的原因在於其高度重複的特性，攻擊者發送大量相似的查詢請求，S-PDFA 能夠識別這種重複模式，將 98,200 筆日誌記錄精煉為僅 5 個核心攻擊模式。相對而言，基線重播攻擊的壓縮比較低 (9:1)，反映其複雜性和多樣性，系統需要保留更多細節以完整呈現攻擊全貌。整體壓縮比 1,089.4:1 展示系統的整體效能，意味著平均每 1,089 個封包可以用一個攻擊圖節點表示。表二詳列各攻擊類型的壓縮比分析。

表二：攻擊類型壓縮比分析表 (Table 2: Compression Ratio Analysis)

攻擊類型	封包數量	攻擊圖數量	壓縮比	備註
Query Flooding	75,678	5	19,640:1	最高壓縮比
Reconnaissance	673	1	673:1	單一行為模式
Write All Coils	495	2	248:1	批次操作
Modify Length	381	3	127:1	簡單模式
False Injection	374	4	94:1	集中攻擊模式
Stack Frames	368	4	92:1	中等複雜度
Baseline Replay	467	53	9:1	多目標分散攻擊
整體總計	**78,436**	**72**	**1,089.4:1**	所有攻擊總計

4.5 實驗二：SCADA HMI 真實攻擊分析

SCADA HMI 資料集的規模為系統帶來顯著挑戰。117 萬個封包、8.3 小時的流量資料不僅考驗處理效能，更重要的是如何從海量資料中提取有意義的攻擊模式。系統採用多層次過濾策略應對此挑戰：在 Zeek 解析階段僅提取安全相關的協定欄位減少資料量；在日誌轉換階段實施積極的去重和聚合，將 134,494 條原始告警壓縮為 15,150 條 (11.3%)；在事件序列生成階段使用時間窗口切分產生 4 個主要事件序列和 6 個子序列。

系統成功處理 117 萬個封包，識別出 5 個主要受害目標，生成 21 張攻擊圖。對 SCADA 主站 (185.175.0.4) 的 7 張攻擊圖展示複雜的多階段攻擊，包含偵察 (T0846)、識別 (T0861)、暴力破解 (T0806)、參數修改 (T0836)、拒絕服務 (T0814)等多種技術。HMI 工作站 (185.175.0.5)共有 6 張攻擊圖，攻擊模式包括 BRUTE_FORCE_IO、DENIAL_OF_SERVICE_ICS、EXPLOITATION_FOR_EVASION 等，顯示對 HMI 的全面滲透策略。PLC 控制器 (185.175.0.8) 的 4 張攻擊圖展現針對性的控制操作，相較於 SCADA 和 HMI，PLC 受到的攻擊種類較少但更為直接，體現工控攻擊最終目標是獲得實體系統的控制權。

實驗二最顯著的成果是實現極高的資料壓縮比。從 100MB 的原始 PCAP 檔案 (包含 1,172,759 個封包)到最終的 21 張攻擊圖 (共 111 個節點)，總體壓縮比達到 55,845:1。多層次的壓縮分析揭示系統在不同抽象層級的精煉能力：封包級壓縮比達到 10,565:1；日誌級壓縮比為 1,550:1；事件級壓縮比為 137:1。這種逐層提煉的過程體現知識萃取的價值，在大幅減少數據量的同時保持攻擊行為的可解釋性。

4.6 綜合分析與系統評估

兩個實驗的對比分析提供系統能力的全面評估。實驗一展示系統對標準化攻擊的處理能力，平均每種攻擊產生 10.3 張攻擊圖，處理時間少於 1 分鐘；實驗二證明系統對真實複雜攻擊的適應性，將 8.3 小時的攻擊濃縮為 21 張關鍵攻擊圖。識別能力方面，兩個實驗都達到 100%的攻擊類型識別率。更重要的是，系統展現良好的泛化能力，實驗二中出現的某些攻擊變體並未包含在實驗一的訓練集中，但系統仍能基於行為特徵正確分類，證明 S-PDFA 學習方法的穩健性。

實驗結果充分展示系統的四大優勢： (1) 自動化程度高：從原始 PCAP 到最終攻擊圖，整個流程無需人工干預； (2) 語意理解深入：系統不僅識別攻擊技術，還理解技術間的邏輯關係； (3) 處理效能優異：面對不同規模的資料集都能在合理時間內完成處理； (4) 結果可解釋性強：生成的攻擊圖包含豐富的上下文資訊，使得非專業人員也能理解攻擊過程。

實驗也揭示系統的某些限制： (1) 對加密流量的處理能力有限，當攻擊流量使用加密或隧道技術時可能無法提取足夠的特徵； (2) 極端情況下的資源消耗，如查詢洪水攻擊的處理時間提示潛在的效能瓶頸； (3) 攻擊圖數量控制問題，基線重播產生的 53 張攻擊圖可能造成資訊過載，需要開發智慧聚合機制。這些限制為未來改進提供明確方向。

伍、結論

本研究成功建構一套基於 Zeek 與 SAGE 整合的工控系統自動化攻擊圖生成系統。實驗結果驗證三項核心發現： (1) 事件抽象化的有效性：四階段轉換流程成功實現從原始封包至語意事件的結構化對應，平均壓縮比達 764:1，顯著降低分析師之資訊負荷；(2) S-PDFA 對低頻攻擊的識別能力：透過後綴導向之模型建構，系統可識別多階段攻擊路徑，並重建攻擊者從初始入侵至最終目標的策略脈絡； (3) 標準化與可解釋性兼備：生成之攻擊圖涵蓋 15 類主要攻擊類型與 83 項 ATT&CK 技術標準，具備語意標註、視覺分層與技術對應性。

本研究之主要技術貢獻包括： (1) Zeek 與 SAGE 整合之三層式分析架構，建構從資料解析、行為建模至視覺化輸出的自動化流程； (2) 事件抽象化機制與語意編碼策略，提出四階段事件轉換流程，實作協定層、行為層與攻擊層之多層語意對應； (3) S-PDFA 模型應用於低頻攻擊行為識別，導入後綴導向的序列學習演算法； (4) MITRE ATT&CK for ICS 自動對應與圖形視覺化技術，建立事件與戰術技術編號之關聯機制。

未來研究可從以下面向延伸： (1) 跨協定擴展與多協定融合，擴展至 DNP3、IEC 61850 等協定； (2) 加密與隧道化通訊之處理機制，探討引入流量模式分析與時間特徵提取技術； (3) 深層時序建模與行為異常預測，導入時間序列分析與異常偵測技術； (4) 動態聚合與視覺壓縮策略，發展基於語意聚類與行為相似度之視覺壓縮技術。總結而言，本研究建構之 Zeek-SAGE 攻擊圖建構系統，具備自動化、標準化與可解釋性三大優勢，為工控系統之威脅分析與決策支援提供一套具實務價值之整合式解決方案。

參考文獻

[1] M. M. Aslam, A. Tufail, R. A. A. H. M. Apong, L. C. De Silva, and M. T. Raza, “Scrutinizing Security in Industrial Control Systems: An Architectural Vulnerabilities and Communication Network Perspective,” *IEEE Access*, vol. 12, pp. 67537-67573, 2024.

[2] S. Chaiyasoonthorn et al., “Cybersecurity for Industrial Control Systems,” in 2024 9th *South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Sept. 2024, pp. 18-24.

[3] C. Phillips and L. P. Swiler, “A graph-based system for network-vulnerability analysis,” *in Proceedings of the 1998 workshop on New security paradigms*, 1998, pp. 71-79.

[4] X. Ou, W. F. Boyer, and M. A. McQueen, “A scalable approach to attack graph generation,” *in Proceedings of the 13th ACM Conference on Computer and Communications Security*, 2006, pp. 336-345.

[5] K. Kaynar, “A taxonomy for attack graph generation and usage in network security,” *Journal*

of Information Security and Applications, vol. 29, pp. 27-56, Aug. 2016.
[6] O. Alexander, M. Belisle, and J. Steele, "MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy," *MITRE Corporation, Technical Report*, Mar. 2020.
[7] The MITRE Corporation, "MITRE ATT&CK® for ICS Matrix, v17," April 2025. [Online]. Available: https://attack.mitre.org/
[8] A. Tiwari, S. Saraswat, U. Dixit, and S. Pandey, "Refinements In Zeek Intrusion Detection System," *in 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Mar. 2022, pp. 974-979.
[9] CISA, "ICSNPP: Industrial Control Systems Network Protocol Parsers," GitHub. [Online]. Available: https://github.com/cisagov/ICSNPP
[10] A. Nadeem, S. Verwer, and S. J. Yang, "SAGE: Intrusion Alert-driven Attack Graph Extractor," *in Symposium on Visualization for Cyber Security (Vizec)*, IEEE, 2021.
[11] A. Nadeem, S. Verwer, S. Moskal, and S. J. Yang, "Alert-Driven Attack Graph Generation Using S-PDFA," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 731-746, Mar. 2022.
[12] K. Boakye-Boateng, A. A. Ghorbani, and A. H. Lashkari, "Securing Substations with Trust, Risk Posture, and Multi-Agent Systems: A Comprehensive Approach," in 2023 20th *Annual International Conference on Privacy, Security and Trust (PST)*, Aug. 2023, pp. 1-12.

[作者簡介]

林子婷，國立臺灣科技大學資訊工程系碩士班研究生。研究領域為工業控制系統安全、網路安全監控與攻擊圖建構技術。

王紹睿，國立臺灣科技大學資訊工程系助理教授。研究領域包括資訊安全、工業控制系統安全、機器學習應用於資安等。