Schema SWaT-KG v0

# 1. Đặt vấn đề và Ý tưởng

Trong các hệ thống công nghiệp hiện đại, dữ liệu được sinh ra từ nhiều lớp khác nhau: cảm biến vật lý, thiết bị chấp hành, bộ điều khiển (PLC), hệ thống SCADA, cũng như nhật ký tấn công mạng. Nếu chỉ lưu trữ rời rạc, việc khai thác và phân tích nguyên nhân–kết quả sẽ rất khó khăn. Do đó, cần một schema chuẩn hóa để gom toàn bộ tri thức vào một Knowledge Graph. Ý tưởng chính của SWaT-KG v0 là mô tả nhà máy xử lý nước SWaT dưới dạng graph đa lớp: Plant → Stage → Sensor/Actuator → FeatureType → Rule/Event → Attack. Schema này cho phép vừa theo dõi vận hành vật lý, vừa kiểm tra logic an toàn, vừa phân tích tấn công cyber-physical.

# 2. Kiến trúc Schema

Kiến trúc của SWaT-KG v0 gồm bốn lớp chính:  
• Plant/Stage: biểu diễn cấu trúc nhà máy gồm 6 giai đoạn xử lý (Raw Water Intake, Pre-treatment, UF, Dechlorination, RO, Storage).  
• Physical layer: mỗi Stage có các tank, module, sensor (LIT, FIT, DPIT) và actuator (pump, motorized valve, UV lamp). FeatureType chuẩn hóa đại lượng đo lường (mực nước, lưu lượng, chênh áp…).  
• Control layer: PLC cho từng stage, SCADA, HMI, Historian, cùng mạng truyền thông hai tầng (Level-0, Level-1). Các SCADA tag ánh xạ tới sensor/actuator, giúp đồng bộ dữ liệu mạng và vật lý.  
• Knowledge & Security layer: Rule và Event mã hóa điều kiện–hành động; Attack/AttackLog mô tả kịch bản tấn công (SSSP, SSMP…).

# 3. Ví dụ minh họa

Ví dụ Stage P1 – Raw Water Intake:  
• Sensor: LIT-101 đo mực nước bồn, FIT-101 đo lưu lượng.  
• Actuator: MV-101 (van), P-101 và P-102 (bơm chính và dự phòng).  
• Procedure FillCycle: Step 1 mở van MV-101 để cấp nước; Step 2 khi LIT-101 đạt mức LL\_OK, khởi động bơm P-101 để bơm sang P2.  
• Rule: nếu LIT-101 ≤ 300 mm, thì tắt P-101 và phát Event EV.P1.LowLevelTrip để bảo vệ bơm.  
  
Ví dụ Stage P3 – Ultrafiltration (UF):  
• Sensor: LIT-301 đo mức, FIT-301 đo lưu lượng, DPIT-301 đo chênh áp.  
• Actuator: bơm P-302, các van MV-301..304.  
• Procedure FilterCycle: Step 1 khởi động P-302 nếu LIT-301 ≥ LL\_OK; Step 2 nếu ΔP cao (DPIT-301 > 0.8 bar) thì kích hoạt backwash (mở van 301/303/304).  
• Rule: HighDPBackwash phát Event EV.P3.BackwashStart (bảo trì).

# 4. Ý nghĩa và Ứng dụng

Schema SWaT-KG v0 mang lại các lợi ích sau:  
• Chuẩn hóa tri thức: gom cấu trúc plant, thiết bị, dữ liệu, luật, và log tấn công vào cùng một graph.  
• Truy vấn dễ dàng: có thể hỏi graph những câu như “Van nào mở khi backwash?”, “Tấn công nào liên quan đến LIT-301?”, “Rule nào bảo vệ bơm P-101?”.  
• Phân tích nguyên nhân–hậu quả: Event, Rule, Attack và Procedure liên kết theo quan hệ → graph causal.  
• Hỗ trợ phát hiện & giải thích bất thường: mapping sensor → feature → rule giúp so sánh dữ liệu đo với logic domain.  
• Ứng dụng bảo mật ICS: Attack node cho phép đánh giá cơ chế phát hiện, gắn nhãn normal/attack cho dữ liệu.  
  
Kết quả: SWaT-KG v0 là nền tảng cho causal discovery + KG verification và anomaly detection trong các hệ thống công nghiệp.