

Ứng dụng Industrial IoT & mô hình Purdue truyền thống.

Hanoi, 19 Dec 2022

Industrial IoT đang chuyển đổi tương lai của các ngành công nghiệp, góp phần tạo nên các nhà máy thông minh. Theo dự báo, quy mô thị trường Industrial IoT toàn cầu dự kiến 112,7 tỷ USD vào năm 2026.

Việt nam cũng nằm trong xu thế đó, triển khai IIoT thực tế tại Việt nam tuy vẫn còn hạn chế, với sự thận trọng trong đầu tư, nhưng cũng đã bắt đầu phát triển, với nhiều hãng cung cấp giải pháp đa dạng.



Hình:Đánh giá chất lượng một hệ thống quan trắc môi trường tại IoTlab

Các ứng dụng chính của IIoT có thể chia làm loại hình như dưới đây, với quan sát thị trường của chúng tôi:

Predictive maintenance Bảo trì dự đoán	Đây là lĩnh vực rất tiềm năng với nhiều story, tuy nhiên thực tế triển khai mới rất hạn chế
Location tracking Giám sát định vị	Hiện đã được dùng rất phổ biến trong lĩnh vực giao thông vận tải, logistics
Workplace analytics Phân tích môi trường làm việc	Còn hạn chế. Các ứng dụng phân tích hành vi nhân viên bán hàng, tình trạng của lái xe đường dài tỏ ra rất tiềm năng.

Remote quality monitoring Giám sát, theo dõi từ xa	Đã phổ biến nhiều trong ngành điện, các trạm điện & nhà máy không người trực tại chỗ.
Energy optimization Tối ưu hóa sử dụng năng lượng	Bắt đầu được ứng dụng cho các nhà máy sản xuất, khu công nghiệp. Khu vực miền nam được ứng dụng nhiều hơn

Trước đây, với chuẩn công nghiệp, kiến trúc hệ thống thường đi theo mô hình Purdue ([Purdue Enterprise Reference Architecture - Wikipedia](#)) với các phân lớp chặt chẽ, hệ thống đóng.

Với IIoT, vấn đề trở nên linh hoạt hơn nhiều, cũng đồng nghĩa với rất nhiều rủi ro về an ninh hệ thống. Điển hình, vào năm 2016, [Mirai \(malware\) - Wikipedia](#) đã lây nhiễm hơn 600.000 thiết bị IoT và gây ra tấn công DDoS trên toàn cầu. Nguyên nhân gây ra bởi việc chủ quan trong việc tuân thủ các nguyên tắc về bảo mật, cấu hình & quản lý các thiết bị IoT đầu cuối.

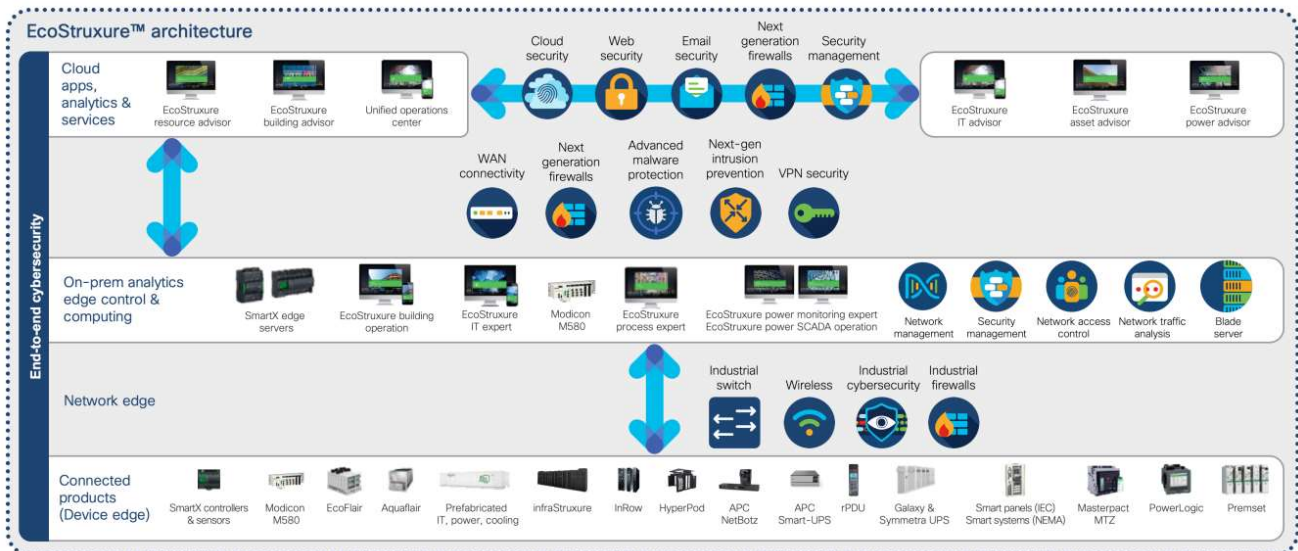
Cũng về vấn đề bảo mật, theo thống kê của Palo Alto Networks, 98% lưu lượng các thiết bị IoT không được mã hóa, 57% các thiết bị IoT cũng dễ bị tấn công ở mức độ nghiêm trọng trung bình hoặc cao.

Vậy câu hỏi đặt ra, ở góc độ kiến trúc tổng thể, khi triển khai Industrial IoT, chúng ta có thể đi theo mô hình nào?

Mô hình Purdue được đưa ra từ những năm 1990, như là một mô hình chuẩn cho các thiết kế công nghiệp, hiện nay vẫn đang được áp dụng trên toàn thế giới. Tuy nhiên, kể từ thời điểm ra đời đến nay, công nghệ & ứng dụng đã có rất nhiều thay đổi, do đó trong nhiều tình huống, mô hình Purdue cũng cần có những thay đổi cho phù hợp.

Điều đó cũng dễ hiểu, khi Industrial IoT Consortium (IIC) ban đầu được thành lập bởi AT&T, Cisco, General Electric, IBM, và Intel vào 2014, hiện nay đã có 159 thành viên. IIC đã đưa ra [Security Framework](#) chi tiết về kiến trúc bảo mật cho hệ thống, tuy vậy cũng không hề nhắc đến Purdue model.

Cisco & Schneider cùng nhau khuyến nghị kiến trúc cho hệ thống hội tụ IT/OT (như hình vẽ dưới), với các mô hình hiện đại như Edge computing, Cloud, thì cũng không nhắc tới Purdue model.



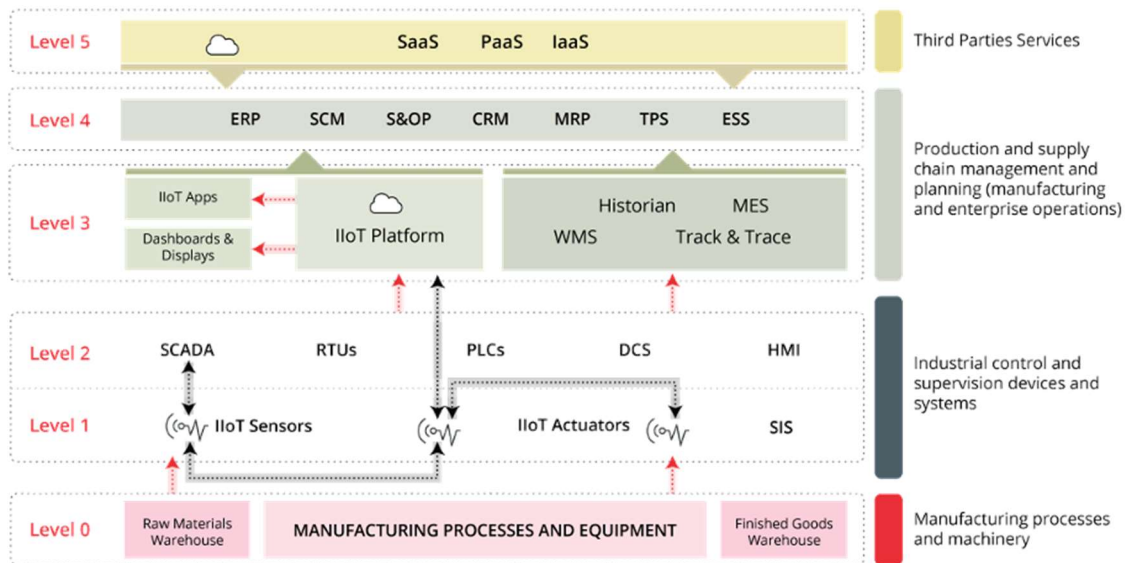
Hình: Kiến trúc chung Schneider - Cisco

Schneider cũng đưa ra khuyến nghị riêng của mình với mô hình Purdue, cho phép các thiết bị IIoT tại các Purdue level có thể nối lên Cloud một cách an toàn.

Như vậy chúng ta có thể thấy nhiều biến thể của Purdue, hoặc các mô hình mới được đưa ra cho phù hợp hơn.

Lựa chọn mô hình nào để triển khai IIoT khiến nhiều doanh nghiệp phải cân nhắc. Với IIoT, data không chỉ đóng kín trong các phân lớp Purdue truyền thống, mà còn đi ra ngoài phạm vi doanh nghiệp, đi lên Cloud. Trong trường hợp này, thì mô hình Purdue đã lạc hậu.

Có nhiều khuyến nghị thay thế, như kiến trúc dưới đây do ENISA (European Union Agency for Cybersecurity) đưa ra. Theo đó, IIoT cloud platform được coi là Level-3, giao tiếp trực tiếp với các thiết bị đầu cuối IIoT tại Level 1. Theo chúng tôi, kiến trúc này là khả thi trong việc kết hợp giữa các mô hình công nghệ mới, với kiến trúc phân lớp công nghiệp truyền thống, vừa đảm bảo tính linh hoạt, đồng thời vẫn giữ được tính bền vững, an toàn hệ thống vốn cần thiết cho các ngành công nghiệp.



Hình: Khuyến nghị của ENISA

Đối với IoTlab, trong các thiết kế cho khách hàng, quan điểm của chúng tôi là vẫn tham khảo mô hình Purdue, ứng dụng khái niệm layers & segmentation của mô hình Purdue, áp dụng các mô hình công nghệ mới, tuân thủ các khuyến nghị an toàn hệ bảo mật công nghiệp ISA 99/IEC 62443.