# YÊU CẦU KỸ THUẬT

## Gói thầu: PTV/2026-09: Thực hiện kiểm tra, đánh giá ATTT cho các hệ thống điều khiển của Công ty Thủy điện Ialy năm 2026

### 1. Giới thiệu chung gói thầu

### 1.1. Thông tin chung:

- Tên gói thầu: PTV/2026-09: Thực hiện kiểm tra, đánh giá ATTT cho các hệ thống điều khiển của Công ty Thủy điện Ialy năm 2026.

- Chủ đầu tư: Công ty Thủy điện Ialy - Chi nhánh Tập đoàn Điện lực Việt Nam.

- Địa điểm thực hiện:

+ Nhà máy Thủy điện Ialy, xã Ya Ly, tỉnh Quảng Ngãi;

+ Nhà máy Thủy điện Ialy mở rộng, xã Ya Ly, tỉnh Quảng Ngãi;

+ Nhà máy Thủy điện Sê San 3, xã Ya Ly, tỉnh Quảng Ngãi;

+ Nhà máy Thủy điện Pleikrông, xã Sa Bình, tỉnh Quảng Ngãi.

### 1.2. Phạm vi kiểm tra, đánh giá ATTT:

Phạm vi kiểm tra, đánh giá ATTT bao gồm toàn bộ các hệ thống điều khiển công nghiệp (OT/ICS/SCADA) đang vận hành tại các Nhà máy Thủy điện của Công ty Thủy điện Ialy, bao gồm: Hệ thống điều khiển phân tán (DCS), Hệ thống giám sát (SCADA) và các chương trình ứng dụng liên quan.

Danh mục thiết bị, chương trình ứng dụng chi tiết như sau:

| Stt | Thiết bị, chương trình ứng dụng | Đơn vị tính | Số lượng |
|---|---|---|---|
| **I** | **Nhà máy Thủy điện Ialy** | | |
| **1** | **Hệ thống DCS** | | |
| 1.1 | Máy chủ<br>- ASCS1/OWS1 Server;<br>- ASCS2/OWS2 Server;<br>- OPC1/HIS1 Server;<br>- OPC2/HIS2 Server | Thiết bị | 04 |
| 1.2 | Máy tính HMI, máy tính vận hành, máy tính kỹ thuật (OWS3, OWS4, EWS, ES) | Thiết bị | 04 |
| 1.3 | Chương trình ứng dụng<br>- Control Builder M<br>- ABB S+ Engineering<br>- ABB Automation Builder 2.1<br>- OptimumC MPC (v2.7)<br>- OptimumC OPC server (v2.0)<br>- Historical Data Server (V2.7) | Chương trình | 06 |
| **2** | **Hệ thống SCADA** | | |
| 2.1 | Máy tính Gateway SCADA | Thiết bị | 01 |

| Stt | Thiết bị, chương trình ứng dụng | Đơn vị tính | Số lượng |
|---|---|---|---|
| 2.2 | Máy tính HMI SCADA HMI | Thiết bị | 01 |
| 2.3 | Ứng dụng SCADA Survalent SmartVU | Chương trình | 01 |
| **II** | **Nhà máy Thủy điện Sê San 3** | | |
| **1** | **Hệ thống DCS** | | |
| 1.1 | Máy chủ<br>- Server1A, SPOSRV1A<br>- Server1B, SPOSRV1B | Thiết bị | 02 |
| 1.2 | Máy tính vận hành, máy tính kỹ thuật<br>SPOWS01, SPOWS02, SPOWS03, SPEWS01, SPEWS. | Thiết bị | 05 |
| 1.3 | Chương trình ứng dụng<br>- ABB S+ Operations History<br>- ABB S+ Operations Display | Chương trình | 02 |
| **2** | **Hệ thống SCADA** | | |
| 2.1 | Ứng dụng SCADA iConf.exe | Chương trình | 01 |
| **III** | **Nhà máy Thủy điện Pleikrông** | | |
| **1** | **Hệ thống DCS** | | |
| 1.1 | Máy chủ<br>- 0CKP01/Server 01,<br>- 0CKP02/Server 02,<br>- 0CKP03/Server HIS. | Thiết bị | 03 |
| 1.2 | Máy tính HMI, máy tính vận hành, máy tính kỹ thuật (OWS1, OWS2, OWS3, EWS, ES) | Thiết bị | 05 |
| 1.3 | Chương trình ứng dụng<br>- Engineering<br>- Historical Data Server | Chương trình | 02 |
| **2** | **Hệ thống SCADA** | | |
| 2.1 | Máy tính Gateway SCADA | Thiết bị | 01 |
| 2.2 | Máy tính HMI SCADA | Thiết bị | 01 |
| 2.3 | Ứng dụng SCADA Survalent SmartVU | Chương trình | 01 |
| **IV** | **Nhà máy Thủy điện Ialy mở rộng** | | |
| 1 | Máy tính chủ cơ sở dữ liệu HT DCS | Thiết bị | 02 |
| 2 | Máy tính màn hình lớn HT DCS | Thiết bị | 01 |
| 3 | Máy tính chủ hệ thống GSTT máy phát | Thiết bị | 01 |
| 4 | Máy tính trạm hệ thống GSTT máy phát | Thiết bị | 01 |
| 5 | Máy tính trạm vận hành HT DCS | Thiết bị | 04 |
| 6 | Máy tính trạm kỹ thuật HT DCS | Thiết bị | 01 |

| Stt | Thiết bị, chương trình ứng dụng | Đơn vị tính | Số lượng |
|---|---|---|---|
| 7 | Máy tính kỹ thuật HT DCS | Thiết bị | 01 |
| 8 | Máy tính hệ thống GSTT MBA | Thiết bị | 01 |
| 9 | Máy tính kỹ thuật HT kích từ, điều tốc | Thiết bị | 04 |
| 10 | Máy tính Điều tốc HIPASE-T | Thiết bị | 04 |
| 11 | Máy tính HT GSTT GIS | Thiết bị | 01 |
| 12 | Chương trình ứng dụng:<br>- SCALA 250 V7.2<br>- HIPASE Engineering Tool<br>- PCM 600<br>- ZOOM Software<br>- Phần mềm HTGS khí SF6 thiết bị GIS<br>- Phần mềm Hệ thống điều khiển DCS cho máy trạm vận hành 800xA<br>- Sicam Device Manager | Chương trình | 07 |

- Thời gian thực hiện: Quý III/2026.

- Tổng thời gian thực hiện dịch vụ: không quá 15 ngày.

**2. Mục tiêu công việc:**

Thực hiện kiểm tra, đánh giá an ninh mạng định kỳ, rà quét mã độc, phát hiện và khắc phục kịp thời các lỗ hổng bảo mật, đánh giá mức độ ảnh hưởng và đề xuất biện pháp xử lý, cập nhật bản vá phù hợp nhằm nâng cao mức độ an toàn thông tin cho hệ thống OT của Công ty Thủy điện Ialy.

**3. Yêu cầu kỹ thuật của gói thầu:**

**3.1. Yêu cầu chung**

Nhà thầu phải thực hiện đầy đủ các nội dung công việc theo phạm vi kiểm tra, đánh giá ATTT và cam kết tuân thủ các yêu cầu sau:

- Bảo mật tuyệt đối toàn bộ dữ liệu, thông tin, tài liệu và cấu hình hệ thống của Chủ đầu tư trước, trong và sau quá trình thực hiện dịch vụ; không được sao chép, lưu trữ, khai thác, tiết lộ hoặc cung cấp cho bất kỳ bên thứ ba nào dưới mọi hình thức khi chưa có sự chấp thuận bằng văn bản của Chủ đầu tư;

- Toàn bộ hoạt động khảo sát, kiểm tra, thu thập thông tin và xác minh trên hệ thống, thiết bị OT phải được thực hiện trực tiếp tại hệ thống/thiết bị; không được truy cập từ xa và không được kết nối HT OT với internet trong quá trình thực hiện;

- Không được kết nối bất kỳ thiết bị lưu trữ hai chiều nào (bao gồm nhưng không giới hạn: USB, ổ cứng di động, thẻ nhớ, điện thoại thông minh, máy tính xách tay, máy tính bảng và các thiết bị tương tự) vào hệ thống OT;

- Không cài đặt bất kỳ phần mềm, công cụ hunting, agent, script hoặc thành phần kỹ thuật nào lên hệ thống OT, đồng thời không thực hiện các thay đổi

Registry, Policy đối với cấu hình, chính sách, dịch vụ hoặc trạng thái thiết bị có khả năng ảnh hưởng đến tính ổn định của hệ thống;

- Tất cả hoạt động kiểm tra, rà quét, giám sát, phân tích và kiểm thử phải tuân thủ nguyên tắc "Zero Impact" và "Safe Assessment", bảo đảm không gây gián đoạn sản xuất, không làm thay đổi cấu hình vận hành và không ảnh hưởng đến tính sẵn sàng của hệ thống OT.

- Toàn bộ dữ liệu, nhật ký (log), kết quả quét, kết quả đánh giá, báo cáo và các thông tin thu thập hoặc trích xuất từ các công cụ đánh giá phải được lưu trữ, bàn giao đầy đủ cho Chủ đầu tư; các dữ liệu này thuộc quyền sở hữu của Chủ đầu tư và là căn cứ phục vụ theo dõi, đối chiếu, điều tra sự cố và nghiệm thu kết quả thực hiện;

- Tất cả các phần mềm sử dụng phải có bản quyền hợp pháp hoặc thuộc quyền sở hữu hợp pháp của nhà thầu. Nhà thầu phải cung cấp đầy đủ tài liệu chứng minh quyền sử dụng hoặc quyền sở hữu khi được yêu cầu;

Mọi hành vi tự ý kết nối thiết bị, cài đặt phần mềm/công cụ, thay đổi cấu hình hệ thống, can thiệp dịch vụ, kết nối Internet, truy cập từ xa hoặc thực hiện các thao tác kỹ thuật khác khi chưa được Chủ đầu tư chấp thuận đều bị xem là vi phạm nghiêm trọng. Chủ đầu tư có quyền đình chỉ ngay việc triển khai, tạm dừng hoặc chấm dứt hợp đồng; đồng thời Nhà thầu phải chịu toàn bộ trách nhiệm khắc phục sự cố, khôi phục hệ thống và bồi thường mọi thiệt hại phát sinh.

**3.2. Yêu cầu kỹ thuật chi tiết:**

**3.2.1. Đánh giá cấu hình:**

Thực hiện rà soát và đánh giá cấu hình toàn bộ thiết bị tại mục **"1.2. Phạm vi kiểm tra, đánh giá ATTT"**, bao gồm:

- Cấu hình an toàn hệ điều hành, phần mềm ứng dụng và firmware;

- Quản lý tài khoản, phân quyền truy cập và xác thực người dùng;

- Cơ chế cập nhật vá lỗi bảo mật và phiên bản phần mềm;

- Cơ chế ghi nhật ký, giám sát và phát hiện sự kiện an toàn thông tin;

- Các dịch vụ, cổng kết nối và ứng dụng đang hoạt động;

- Các thiết lập an toàn khác liên quan đến vận hành hệ thống OT.

Kết quả đánh giá phải xác định rõ các điểm yếu bảo mật, mức độ rủi ro và khuyến nghị biện pháp khắc phục.

**3.2.2. Kiểm tra mã độc và lỗ hổng bảo mật:**

**a. Kiểm tra mã độc**

- Sử dụng thiết bị, công cụ chuyên dụng để rà quét, phát hiện mã độc, Rootkit và các dấu hiệu tấn công nâng cao (APT/TTP) trên hệ thống OT.

- Công cụ rà quét phải hoạt động theo dạng Portable/Standalone;

- Việc chuyển mẫu mã độc hoặc tệp nghi ngờ mã độc ra ngoài phân tích phải thực hiện thông qua thiết bị truyền dữ liệu một chiều (ví dụ như: Data

Diode/Unidirectional Gateway) hoặc giải pháp kỹ thuật tương đương được Chủ đầu tư chấp thuận.

**b) Rà quét lỗ hổng bảo mật**

- Sử dụng thiết bị hoặc công cụ rà quét chuyên dụng có tích hợp sẵn cơ sở dữ liệu nhận diện lỗ hổng CVE (Common Vulnerabilities and Exposures - Hệ thống danh mục lỗ hổng bảo mật quốc tế) được cập nhật mới nhất trong vòng 60 ngày (dạng Offline).

- Tất cả lỗ hổng mức Nghiêm trọng (Critical) và Cao (High) phải được phân tích nguyên nhân, đánh giá ảnh hưởng và đề xuất phương án xử lý.

**c) Cập nhật bản vá bảo mật**

- Nhà thầu có trách nhiệm rà soát, đánh giá mức độ phù hợp và khả năng tương thích trước khi thực hiện cập nhật các bản vá bảo mật do nhà sản xuất phát hành miễn phí đối với hệ điều hành, phần mềm ứng dụng, firmware và các thành phần liên quan của hệ thống OT.

- Việc cập nhật bản vá chỉ được thực hiện đối với các bản vá phù hợp với hiện trạng hệ thống và theo đúng khuyến cáo của nhà sản xuất, bảo đảm không ảnh hưởng đến tính ổn định, độ tin cậy và khả năng vận hành liên tục của hệ thống điều khiển.

- Mọi hoạt động cập nhật bản vá phải được giám sát của Chủ đầu tư chấp thuận trước khi thực hiện. Nhà thầu phải lưu vết đầy đủ trạng thái hệ thống trước và sau khi cập nhật bằng hình ảnh vào nhật ký thi công để làm căn cứ nghiệm thu.

**3.2.3. Kiểm thử xâm nhập và truy vết tấn công:**

- Thực hiện kiểm thử xâm nhập theo phương pháp Black-box và Gray-box, tuân thủ nguyên tắc Safe Pentest;

- Giám sát lưu lượng mạng, phân tích nhật ký (log), truy vết hoạt động bất thường và rà soát toàn diện hệ thống nhằm phát hiện các dấu hiệu tấn công có chủ đích (APT), mã độc, kết nối trái phép, dịch vụ hoặc tiến trình bất thường có nguy cơ ảnh hưởng đến an toàn vận hành hệ thống OT;

- Kết quả thực hiện phải có đủ bằng chứng tổng hợp trong báo cáo đánh giá an toàn thông tin phục vụ công tác nghiệm thu.

**3.3. Yêu cầu thiết bị và công cụ:**

**3.3.1. Thiết bị:**

Sử dụng thiết bị chuyên dụng phục vụ đánh giá an toàn thông tin, bảo đảm sạch mã độc, không chứa dữ liệu không liên quan đến phạm vi công việc và được cách ly hoàn toàn với Internet trong suốt quá trình thực hiện dịch vụ.

**3.3.2. Công cụ:**

Công cụ rà quét lỗ hổng phải:

- Phải được tích hợp sẵn cơ sở dữ liệu nhận diện lỗ hổng quốc tế (CVE);

- Có khả năng phân tích sâu gói tin (Deep Packet Inspection - DPI), nhận diện chính xác các giao thức công nghiệp tối thiểu gồm: IEC 60870-5-104,

Modbus TCP, OPC, OPC DA/UA, DNP3 và phát hiện các kết nối trái phép, hành vi bất thường trong mạng OT từ Level 0 đến Level 4.

**3.4. Yêu cầu nhân sự, năng lực và kinh nghiệm:**

Yêu cầu về nhân sự chủ chốt được trình bày tại Bảng số 02: Yêu cầu về nhân sự chủ chốt (Webform trên Hệ thống), mục 2.2 thuộc Chương III. TIÊU CHUẨN ĐÁNH GIÁ E-HSDT.

**3.5. Yêu cầu về năng lực tổ chức cung cấp dịch vụ:**

- Có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trong đó có đăng ký dịch vụ: Cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng;

- Yêu cầu về kinh nghiệm được trình bày tại Bảng số 01 (Webform trên Hệ thống), mục 2.1 thuộc Chương III. TIÊU CHUẨN ĐÁNH GIÁ E-HSDT

**4. Giải pháp và phương pháp luận:**

Nhà thầu có trách nhiệm xây dựng và trình Chủ đầu tư phương án kỹ thuật, quy trình thực hiện và các biện pháp bảo đảm an toàn thông tin. Phương án phải đáp ứng đầy đủ các yêu cầu kỹ thuật của gói thầu, đồng thời bảo đảm an ninh mạng và duy trì tính ổn định, an toàn tuyệt đối cho hệ thống OT.

**4.1. Phương pháp luận và tiêu chuẩn áp dụng:**

- Phương án kỹ thuật phải được xây dựng trên cơ sở các tiêu chuẩn, quy chuẩn, đảm bảo an toàn thông tin cho hệ thống OT/ICS/SCADA, bao gồm: TCVN 14423:2025, IEC 62443, NIST SP 800-82, ISO/IEC 27001, ISO/IEC 27002, PTES/OSSTMM;

- Quy trình triển khai tối thiểu gồm 06 giai đoạn:

+ Chuẩn bị và khảo sát;

+ Thu thập thông tin;

+ Phân tích lỗ hổng;

+ Kiểm thử có kiểm soát;

+ Khắc phục và cập nhật bản vá;

+ Hậu kiểm và đánh giá lại.

- Mỗi giai đoạn phải được mô tả: Phương pháp thực hiện, thiết bị và công cụ sử dụng, phương án kiểm soát rủi ro.

**4.2. Kế hoạch công tác:**

Nhà thầu phải xây dựng kế hoạch triển khai chi tiết cho từng hệ thống OT, trong đó mô tả rõ:

- Phạm vi và trình tự thực hiện;

- Tiến độ thực hiện;

- Thiết bị, công cụ sử dụng;

- Biện pháp kiểm soát;

- Phương án xử lý sự cố và khôi phục hệ thống (rollback).

Kế hoạch phải bảo đảm không ảnh hưởng đến an toàn vận hành, tính sẵn sàng và độ ổn định của hệ thống OT trong suốt quá trình triển khai dịch vụ.

**5. Quy định về triển khai và nghiệm thu sản phẩm:**

**5.1. Tổ chức triển khai**

Trong thời hạn tối đa 05 ngày làm việc kể từ ngày hợp đồng có hiệu lực, Nhà thầu phải trình Chủ đầu tư kế hoạch triển khai chi tiết để xem xét, chấp thuận trước khi thực hiện.

**5.2. Báo cáo**

Nội dung báo cáo tối thiểu bao gồm:

- Kết quả đánh giá cấu hình an toàn hệ điều hành, phần mềm ứng dụng, cơ chế quản lý tài khoản, phân quyền truy cập, cập nhật bản vá và các dịch vụ đang hoạt động trên hệ thống;

- Kết quả rà quét, phát hiện mã độc, lỗ hổng bảo mật, phân tích nguyên nhân, đánh giá mức độ ảnh hưởng và đề xuất biện pháp khắc phục. Đối với các lỗ hổng mức Nghiêm trọng (Critical) và Cao (High), phải có khuyến nghị xử lý cụ thể;

- Kết quả phân tích lưu lượng mạng, nhật ký và các dấu hiệu bất thường liên quan đến an toàn thông tin, bao gồm kết nối trái phép, mã độc hoặc nguy cơ tấn công có chủ đích (APT);

- Danh mục các bản vá bảo mật đã được cập nhật (nếu có), kết quả thực hiện và đánh giá sau cập nhật;

- Hình ảnh hiện trường, nhật ký thi công, kết quả trích xuất từ các công cụ đánh giá và các tài liệu chứng minh khác phục vụ công tác nghiệm thu.

**5.3. Thành phần hồ sơ nghiệm thu (05 bộ)**

Bàn giao 05 bộ hồ sơ hoàn chỉnh (bản cứng và bản mềm), bao gồm:

- Nhật ký thi công;

- Báo cáo đánh giá an toàn thông tin theo quy định tại Mục 5.2;

- Báo cáo hoàn thành dịch vụ của nhà thầu;

- Biên bản nghiệm thu khối lượng công việc hoàn thành./.