YÊU CẦU VỀ 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:

- 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.

- Phạm vi hệ thống đánh giá: Các hệ thống điều khiển công nghiệp (OT/ICS/SCADA) đang vận hành tại các Nhà máy Thủy điện của Công ty, bao gồm: Hệ thống DCS; Hệ thống SCADA; Máy chủ điều khiển; Máy trạm vận hành (HMI/OWS); Máy trạm kỹ thuật (Engineering Workstation); Thiết bị mạng công nghiệp; Các phần mềm điều khiển và phần mềm hỗ trợ vận hành. Khối lượng thiết bị/chương trình ứng dụng như liệt kê dưới đây:

Stt	Thiết bị	Đơn vị tính	Số lượng
I	**Nhà máy Thủy điện Ialy**		
1	**Hệ thống DCS**		
1.1	Máy chủ - ASCS1/OWS1 Server; - ASCS2/OWS2 Server; - OPC1/HIS1 Server; - 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 - Control Builder M - ABB S+ Engineering - ABB Automation Builder 2.1 - OptimumC MPC (v2.7) - OptimumC OPC server (v2.0) - Historical Data server (V2.7)	Chương trình	06
2	**Hệ thống SCADA**		
2.1	Máy tính Gateway SCADA	Thiết bị	01

Stt	Thiết bị	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 - Server1A, SPOSRV1A - Server1B, SPOSRV1B	Thiết bị	02
1.2	Máy tính vận hành, máy tính kỹ thuật SPOWS01, SPOWS02, SPOWS03, SPEWS01, SPEWS.	Thiết bị	05
1.3	Chương trình ứng dụng - ABB S+ Operations History - 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 - 0CKP01/Server 01, - 0CKP02/Server 02, - 0CKP03/Server HIS.	Thiết bị	03
1.2	Máy tính HMI, máy tính vận hành, máy tính kỹ thuật, máy tính xách tay OWS1, OWS2, OWS3, EWS, ES	Thiết bị	05
1.3	Chương trình ứng dụng - Engineering - Historial 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 (Dell Power Edge R550 Server, Windows Server 2022 Standard)	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

Stt	Thiết bị	Đơn vị tính	Số lượng
4	Máy tính trạm hệ thống GSTT máy phát	Thiết bị	01
5	Máy tính trạm vận hành HT DCS (Dell Precision T5820, Windows 11 22H1 Pro)	Thiết bị	04
6	Máy tính trạm kỹ thuật HT DCS	Thiết bị	01
7	Máy tính kỹ thuật HT DCS (Dell Latitude 5421, Windows 10 Professional 64Bit)	Thiết bị	01
8	Máy tính hệ thống GSTT MBA (Dell Precision 5820, Windows 10 Pro)	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: - SCALA 250 V7.2 - HIPASE Engineering Tool - PCM 600 - ZOOM Software - Phần mềm HTGS khí SF6 thiết bị GIS - Phần mềm Hệ thống điều khiển DCS cho máy trạm vận hành 800xA - Sicam Device Manager	Chương trình	07

- 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 và tầm soát mã độc định kỳ; đồng thời chủ động nhận diện lỗ hổng, cập nhật bản vá lỗi hệ thống và thực hiện kiểm thử xâm nhập nhằm đảm bảo 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 về bảo mật và vận hành:

- Nhà thầu cam kết bằng văn bản chịu trách nhiệm bảo mật toàn bộ dữ liệu và thông tin của hệ thống trong suốt quá trình thực hiện dịch vụ, không tiết lộ hoặc chia sẻ thông tin cho bất kỳ bên thứ ba nào dưới bất kỳ hình thức nào, đồng thời không cài đặt, không để lại bất kỳ phần mềm, công cụ, mã lệnh, script, agent hoặc thành phần kỹ thuật nào trên hệ thống của Chủ đầu tư.

- Trong quá trình kiểm tra, đánh giá hệ thống, Nhà thầu phải tuân thủ các quy định sau:

+ Công tác kiểm tra phải thực hiện trực tiếp tại các Nhà máy Thủy điện, không truy cập từ xa và không kết nối Internet vào hệ thống OT.

+ Không được kết nối thiết bị cá nhân (laptop, ổ cứng di động) hoặc bất kỳ

thiết bị lưu trữ hai chiều nào vào hệ thống OT.

+ Không được thay đổi Registry, Policy, cấu hình hệ thống, trạng thái thiết bị, không vô hiệu hóa dịch vụ hoặc thực hiện bất kỳ thao tác nào có thể gây treo dịch vụ, gián đoạn điều khiển, đặc biệt đối với luồng dữ liệu điều khiển thời gian thực.

+ Tuân thủ nguyên tắc không can thiệp hệ thống (Zero-Impact). Tuyệt đối không cài đặt, triển khai hoặc thực thi bất kỳ phần mềm, công cụ hunting, tool/script, agent nào trực tiếp trên các máy chủ, máy trạm vận hành và máy giao diện HMI.

+ Nhà thầu chỉ được thực hiện các thao tác kỹ thuật sau khi đã xây dựng kế hoạch khôi phục nguyên trạng (Rollback) và được Chủ đầu tư đồng ý; mọi thao tác phải thực hiện thông qua máy trung gian dưới sự kiểm soát quyền truy cập đặc quyền và giám sát của Chủ quản hệ thống.

- Mọi hành vi tự ý kết nối thiết bị lưu trữ hai chiều hoặc thực cài đặt Script/Tool lên hệ thống khi chưa có sự chấp thuận của Chủ đầu tư bị coi là vi phạm an toàn vận hành nghiêm trọng. Chủ đầu tư có quyền đình chỉ hợp đồng ngay lập tức, đồng thời Nhà thầu phải chịu hoàn toàn trách nhiệm khắc phục sự cố và bồi thường toàn bộ thiệt hại (nếu có).

3.2. Yêu cầu kỹ thuật chi tiết:

3.2.1. Đánh giá cấu hình:

Thực hiện rà soát và đánh giá cấu hình an toàn đối với toàn bộ thiết bị mạng công nghiệp, hệ thống HMI và các trạm kỹ thuật nhằm phát hiện các cấu hình chưa phù hợp có thể gây mất an toàn cho hệ thống điều khiển. Nội dung đánh giá bao gồm kiểm tra mức độ tuân thủ các yêu cầu bảo mật đối với hệ điều hành, phần mềm điều khiển và firmware của thiết bị, như cấu hình tài khoản và phân quyền truy cập, các dịch vụ đang hoạt động, cơ chế cập nhật và vá lỗi bảo mật, cũng như các thiết lập an toàn khác trước khi tiến hành kiểm tra, đánh giá ATTT cho hệ thống.

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

- Sử dụng công cụ chuyên dụng (phần mềm rà quét chỉ được chạy từ bên trong thiết bị) để phát hiện mã độc, Rootkit, các kỹ thuật tấn công nâng cao (Memory Injection, DLL Hijacking) mà không được phép cài đặt phần mềm lên các máy tính của hệ thống OT.

- Các mẫu mã độc, hoặc nghi ngờ là mã độc, phải được lưu lại như một phần của báo cáo, việc chuyển các mẫu này ra ngoài phải đảm bảo thực hiện bằng các thiết bị truyền dữ liệu một chiều (Data Diode/Unidirectional Gateway).

- Thực hiện rà soát và dò quét lỗ hổng bảo mật bằng các công cụ chuyên dụng theo chuẩn CVE nhằm phát hiện điểm yếu trên hệ điều hành, phần mềm ứng dụng, firmware cũng như toàn bộ môi trường IT và các giao thức OT đặc thù như Modbus, DNP3, IEC-104.

- Thực hiện cập nhật các bản vá lỗi (Hotfix/Service Pack) cho hệ điều hành và thiết bị mà hãng đã phát hành miễn phí sau khi đã kiểm tra tính tương thích trong môi trường cô lập có kiểm soát.

- Thực hiện Backup cấu hình và dữ liệu hệ thống trước khi tiến hành cập nhật để đảm bảo khả năng khôi phục nguyên trạng (Rollback) nếu xảy ra lỗi.

3.2.3. Kiểm thử xâm nhập có kiểm soát:

- Kiểm thử xâm nhập (Pentest), thực hiện các kịch bản tấn công giả lập không xâm lấn (Black-box, Gray-box) để chứng minh lỗ hổng mà không gây hại cho hệ thống.

- Giám sát sự cố, triển khai giải pháp giám sát và phát hiện xâm nhập SIEM tạm thời để thu thập và phân tích nhật ký (log) trên đường truyền nhằm phát hiện các hành vi bất thường hoặc tấn công APT.

3.2.4. Kiểm thử xâm nhập và dấu vết tấn công:

- Thực hiện kiểm thử xâm nhập từ bên trong để đánh giá khả năng phòng thủ của hệ thống khi có tác nhân nội bộ hoặc mã độc lây lan.

- Rà soát toàn diện các kết nối và tiến trình lạ đang chạy ngầm trong mạng OT để triệt tiêu mọi nguy cơ tiềm ẩn.

3.3. Yêu cầu thiết bị và công cụ hỗ trợ:

Để đảm bảo an toàn tuyệt đối cho hệ thống điều khiển (OT) cấp độ 4, Nhà thầu bắt buộc phải trang bị và sử dụng các nhóm giải pháp công nghệ sau:

3.3.1. Thiết bị:

- Sử dụng thiết bị chuyên dụng một chiều (Unidirectional Data Diode) vật lý thực thụ, Mọi dữ liệu trích xuất từ mạng OT (log, file cấu hình, dữ liệu quét) để phục vụ phân tích phải được thực hiện qua thiết bị Data Diode vật lý chuyên dụng. Đảm bảo dữ liệu chỉ đi ra một chiều duy nhất. Tuyệt đối không sử dụng USB, ổ cứng di động hoặc đĩa quang kết nối trực tiếp vào các máy chủ, máy trạm vận hành. Điều này nhằm triệt tiêu nguy cơ lây nhiễm mã độc ngược từ thiết bị của nhà thầu vào hệ thống OT.

- Sử dụng máy tính chuyên dụng có cấu hình mạnh, được cài đặt các hệ điều hành và phần mềm chuyên dụng cho đánh giá ATTT (Pentest OS), hoàn toàn sạch mã độc và được cách ly hoàn toàn với môi trường Internet.

3.3.2. Công cụ:

- Các công cụ rà quét mã độc chuyên sâu có khả năng phân tích tệp tin, tiến trình và bộ nhớ hệ thống mà không được phép cài đặt (Agentless), hỗ trợ nhận diện các loại mã độc đặc thù tấn công vào hạ tầng năng lượng;

- Phần mềm phải thực thi trực tiếp từ thiết bị chuyên dụng của Nhà thầu (Portable/Standalone). Tuyệt đối cấm cài đặt (Install), sao chép (Copy) hoặc chạy các công cụ hunting, tool/script, agent can thiệp trực tiếp vào Registry, tệp tin hệ thống hoặc tiến trình của máy chủ, máy trạm HMI. Ngăn ngừa xung đột phần

mềm, lỗi màn hình xanh (BSOD) và đảm bảo tính nguyên vẹn của hệ thống OT.

- Công cụ đánh giá lỗ hổng mạng công nghiệp phải sở hữu cơ sở dữ liệu lỗi (Knowledge base) cập nhật, hỗ trợ đầy đủ các giao thức OT (Modbus, DNP3, IEC 61850...) và có tính năng quét an toàn không gây treo thiết bị điều khiển;

- Hệ thống giám sát và phân tích lưu lượng (Traffic Analyzer) có khả năng phân tích gói tin chuyên sâu (DPI) để phát hiện các hành vi bất thường, các kết nối lạ trên đường truyền tín hiệu giữa các tầng Level 0 đến Level 4;

- Công cụ phải tuân thủ mô hình bảo mật Zero Trust, áp dụng cơ chế xác minh liên tục, kiểm soát truy cập theo quyền tối thiểu, đồng thời đảm bảo quá trình đánh giá không gây tác động, không ghi ngược dữ liệu trái phép lên hệ thống mục tiêu;

- Tất cả các công cụ (rà quét mã độc - Agentless, rà quét lỗ hổng công nghiệp, giám sát và phân tích lưu lượng mạng - SIEM) nêu trên phải có giấy phép bản quyền hợp pháp, còn hiệu lực sử dụng tại thời điểm triển khai, hoặc nhà thầu là chủ sở hữu hợp pháp của sản phẩm/công cụ tự phát triển. Nhà thầu phải cung cấp tài liệu chứng minh bản quyền hoặc quyền sở hữu trí tuệ (license, hợp đồng, chứng nhận quyền tác giả, cam kết sở hữu sản phẩm) khi Chủ đầu tư yêu cầu.

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:

Để đảm bảo an toàn tuyệt đối cho hệ thống điều khiển đặc thù, Nhà thầu phải chứng minh năng lực sau:

3.5.1. Pháp lý:

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.

3.5.2. Kinh nghiệm:

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 phải đệ trình phương án kỹ thuật tổng thể và phương pháp luận thực hiện dịch vụ, bảo đảm đáp ứng đầy đủ các nội dung quy định, đồng thời đảm bảo an ninh mạng và duy trì tính ổn định, an toàn tuyệt đối cho hệ thống OT:

4.1. Giải pháp và phương pháp luận:

- Phương pháp luận tổng thể: Phương pháp luận thực hiện được xây dựng trên cơ sở hợp nhất các tiêu chuẩn an toàn thông tin và an ninh hệ thống điều khiển công nghiệp nghiêm ngặt, bao gồm: TCVN 14423:2025, NIST SP 800-82 (Bảo

mật hệ thống điều khiển công nghiệp), IEC 62443 cùng các chuẩn kiểm thử chuyên dụng như PTES/OSSTMM đối với hoạt động kiểm thử có kiểm soát;

- Tiêu chuẩn và khung tham chiếu: Toàn bộ quá trình đánh giá phải được đối soát và thực hiện theo các khung tiêu chuẩn quốc tế và trong nước mới nhất như: TCVN 14423:2025, IEC 62443, NIST Cybersecurity Framework (CSF), ISO/IEC 27001 và ISO/IEC 27002;

- Quy trình triển khai: Hoạt động đánh giá được thực hiện theo quy trình 06 giai đoạn, bao gồm: Chuẩn bị → Thu thập thông tin → Phân tích lỗ hổng → Kiểm thử khai thác có kiểm soát → Khắc phục/Cập nhật bản vá → Hậu kiểm;

Mỗi giai đoạn phải được mô tả chi tiết về phương pháp thực hiện, thiết bị và công cụ sử dụng, đồng thời xác định rõ phương án xử lý rủi ro trước khi triển khai.

4.2. Kế hoạch công tác:

- Nhà thầu phải xây dựng kế hoạch công tác chi tiết, xác định rõ phạm vi công việc, danh mục hạng mục mục tiêu và mốc thời gian hoàn thành cho từng giai đoạn triển khai;

- Thiết lập lộ trình triển khai cụ thể theo từng bước, xác định rõ danh mục thiết bị hỗ trợ, công cụ kỹ thuật chuyên dụng và giải pháp kỹ thuật phù hợp với đặc thù của môi trường mạng OT;

- Phân bổ đội ngũ chuyên gia có năng lực và kinh nghiệm phù hợp, bao gồm các nhân sự có trình độ tương đương nhân sự chủ chốt, nhằm bảo đảm tiến độ thực hiện, chất lượng kỹ thuật và an toàn cho hệ thống trong suốt quá trình triển khai;

- Phương án kỹ thuật phải bảo đảm hệ thống OT duy trì hoạt động ổn định, an toàn và liên tục, không gây gián đoạn đến hoạt động vận hành trong toàn bộ quá trình đánh giá;

- Thiết lập cơ chế kiểm soát chặt chẽ luồng trao đổi dữ liệu giữa môi trường IT và OT; đồng thời triển khai các biện pháp phòng vệ chủ động nhằm phát hiện, ngăn chặn và giảm thiểu các mối đe dọa từ bên ngoài đối với mạng điều khiển công nghiệp;

- Thiết lập quy trình thông tin liên lạc và phối hợp rõ ràng với Chủ đầu tư; kịp thời thông báo, báo cáo và đề xuất phương án xử lý khi phát hiện lỗ hổng nghiêm trọng hoặc các sự cố bất thường trong hệ thống.

4.3. Phê duyệt phương án thi công:

Trong thời hạn tối đa 03 ngày kể từ ngày ký hợp đồng, Nhà thầu bắt buộc phải đệ trình Phương án thi công và Kế hoạch tiến độ chi tiết cho từng hệ thống OT. Mọi hoạt động triển khai tại hiện trường chỉ được phép bắt đầu khi có văn bản phê duyệt chính thức từ Chủ đầu tư.

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Nhà thầu có trách nhiệm thực thi quy trình nghiệm thu minh bạch và tuân

thủ tuyệt đối các tiêu chuẩn bảo mật theo đúng lộ trình đã cam kết:

5.1. Tiêu chuẩn báo cáo kết quả đánh giá và bảo mật dữ liệu

- Báo cáo đánh giá ATTT phải được lập chuyên nghiệp, trực quan, có giá trị thực thi cao và tuân thủ tuyệt đối các nguyên tắc về chủ quyền thông tin, cụ thể bao gồm:

- Trình bày chi tiết phương pháp, công cụ sử dụng và kết quả cập nhật bản vá lỗi. Mọi điểm yếu bảo mật phải được định danh rõ ràng, minh chứng bằng hình ảnh khai thác thực tế tại hiện trường.

- Các lỗ hổng phải được phân loại theo 04 mức độ chuẩn hóa: Nghiêm trọng, Cao, Trung bình, Thấp. Nhà thầu phải đề xuất giải pháp và cam kết khắc phục, trong đó thiết lập thứ tự ưu tiên xử lý ngay các rủi ro Cao và Nghiêm trọng nhằm tối ưu hóa nguồn lực cho Công ty.

- Toàn bộ thông tin, dữ liệu và log quét thu thập được trong quá trình đánh giá là tài sản thuộc quyền sở hữu tuyệt đối của Công ty Thủy điện Ialy. Nhà thầu cam kết không sao chép, không lưu giữ bất kỳ dữ liệu nào liên quan đến hệ thống OT sau khi hoàn tất nghĩa vụ bàn giao, đảm bảo an toàn thông tin tuyệt đối cho Chủ đầu tư.

5.2. Thành phần hồ sơ nghiệm thu (05 bộ)

Nhà thầu tiến hành bàn giao 05 bộ hồ sơ hoàn chỉnh (bao gồm bản cứng và bản mềm), như sau:

- Nhật ký công việc hiện trường: Ghi chép nhật trình chi tiết các thao tác kỹ thuật và biến động hệ thống hàng ngày.

- Báo cáo kết quả đánh giá ATTT (đáp ứng các tiêu chuẩn tại Mục 5.1).

- Biên bản nghiệm thu khối lượng và tiến độ công việc hoàn thành.

- Báo cáo hoàn thành công tác cung cấp dịch vụ của Nhà thầu.

- Toàn bộ bản ghi nhật ký (log) hệ thống và kết quả quét thô (raw data) trích xuất từ các công cụ đánh giá./.