



## Call for Experts

### JWG MTP Security and Runtime Interoperability

Highly volatile markets require a shift in thinking from monolithic plants designed to produce for several decades to modular and flexible solutions. The focus is on speed and efficiency, which can only be achieved through a plug-and-produce concept. The basic idea is to compose plants from intelligent, pre-tested units. Automation technology plays a major role in the realization. From the perspective of automation, the foundation is the creation of a manufacturer-neutral interface that enables the integration of the units, called Process Equipment Assemblies (PEA) into a Process Orchestration Layer (POL). This is where MTP comes in and defines the necessary interface specification, which consists of a defined behavior and a description of the data and functionality provided by the PEA. This ensures interoperability between different manufacturers.

The increasing threat landscape with rising cyberattacks on critical infrastructure, combined with emerging regulations such as the EU Cyber Resilience Act and NIS2 Directive, make comprehensive security specifications essential for productive MTP deployment. Without standardized security mechanisms, each implementation would require custom solutions, undermine the plug-and-produce vision and create potential vulnerabilities.

The JWG MTP Security and Runtime Interoperability will develop aspects like:

- Digital Package Signature for MTP – Cryptographic signing of MTP packages for authenticity and integrity verification
- OPC UA Security for Single Server Equipment – Security requirements for OPC UA communication including authentication, encryption, and certificate management
- Multi Server Equipment Concept – Architectural patterns for PEAs utilizing multiple OPC UA servers
- Security for Multi Server Equipment Concept – Security models for multi-server scenarios including trust relationships and secure inter-server communication
- Security Mechanisms Inside the PEA – Internal security measures such as secure boot, integrity verification, and protection against unauthorized modifications

The JWG will be led by Marwin Madsen, Karlsruhe Institute of Technology.

Specialists from automation suppliers, device manufacturers, operators, module manufacturers, and cybersecurity experts are highly welcome.

**The common kick-off meeting of the Joint Working Group will be held as web meeting on February 4<sup>th</sup>, 1:00 pm to 3:00 pm.**

**Please send registrations until February 1<sup>st</sup>, 2026** directly to the working group leader [marwin.madsen@kit.edu](mailto:marwin.madsen@kit.edu).



## Call for Experts

### JWG MTP Security and Runtime Interoperability

Hochvolatile Märkte erfordern ein Umdenken von monolithischen Anlagen, die auf mehrere Jahrzehnte ausgelegt sind, hin zu modularen und flexiblen Lösungen. Dabei stehen Geschwindigkeit und Effizienz im Vordergrund, was nur durch ein Plug-and-Produce-Konzept erreicht werden kann. Neben dem konstruktiven Aufbau der Anlage spielt vor allem die Automatisierungstechnik eine wesentliche Rolle bei der Zusammenschaltung der Gesamtanlage, so müssen manuelle Integrationsschritte überwunden werden, um einen Geschwindigkeitsvorteil zu erreichen. Die Basis ist dabei die Schaffung einer herstellernerutralen Schnittstelle, die die automatisierungstechnische Integration der einzelnen Process Equipment Assemblies (PEA) in ein Process Orchestration Layer (POL) ermöglicht. An dieser Stelle setzt MTP an und definiert die notwendige Schnittstellenspezifikation, die sich aus einem definierten Verhalten und einer Beschreibung der bereitgestellten Daten zusammensetzt und damit die Interoperabilität zwischen unterschiedlichen Herstellern gewährleistet.

Die zunehmende Bedrohungslage mit steigenden Cyberangriffen auf kritische Infrastrukturen in Verbindung mit neuen Vorschriften wie dem EU-CRA und der NIS2-Richtlinie machen umfassende Securityspezifikationen für einen produktiven MTP-Einsatz unerlässlich. Ohne standardisierte Securitymechanismen würde jede Implementierung maßgeschneiderte Lösungen erfordern, die Plug-and-Produce-Vision untergraben und potenzielle Schwachstellen schaffen.

Die JWG MTP Security and Runtime Interoperability wird Aspekte wie die folgenden entwickeln:

- Digitale Paketsignatur für MTP – Kryptografische Signatur von MTP-Paketen zur Überprüfung der Authentizität und Integrität
- OPC UA Security für Single Server Equipment – Securityanforderungen für die OPC UA Kommunikation, einschließlich Authentifizierung, Verschlüsselung und Zertifikatsverwaltung
- Multi-Server-Gerätekonzept – Architekturmuster für PEAs, die mehrere OPC UA-Server nutzen
- Security für das Multi-Server-Gerätekonzept – Securitymodelle für Multi-Server-Szenarien, einschließlich Vertrauensbeziehungen und sicherer Kommunikation zwischen Servern
- Securitymechanismen innerhalb der PEA – Interne Securitymaßnahmen wie sicherer Start, Integritätsprüfung und Schutz vor unbefugten Änderungen

Die JWG wird von Marwin Madsen vom Karlsruher Institut für Technologie geleitet.

Spezialisten von Automatisierungsanbietern, Geräteherstellern, Betreibern, Modulherstellern und Cybersicherheitsexperten sind herzlich willkommen.

**Die gemeinsame Auftaktveranstaltung der Joint Working Group findet am 4. Februar von 13:00 bis 15:00 Uhr als Web-Meeting statt.**

**Bitte senden Sie Ihre Anmeldungen bis zum 1. Februar 2026 direkt an den Leiter der Arbeitsgruppe [marwin.madsen@kit.edu](mailto:marwin.madsen@kit.edu).**