PRECISE SYSTEMS'
EMITTER FINGERPRINTING

Y-STN and **INT-PAS** are cutting edge AI/ML applications that analyze the features of a signal capture to enable classification of the propagating emitter. Emitter fingerprinting entails the analysis of the signal to identify features that have been introduced through hardware anomalies in the actual emitter instance. For example, oscillator drift, gain mismatch, out of band emissions and other hardware characteristics are unique to the propagating emitter, introducing unique features to the signal that can be analyzed to determine the individual transmitting device, like fingerprints being utilized to identify individual people.

ENABLING TECHNOLOGIES: Emitter fingerprinting requires technologies that can both aid research and development in the identification of emitter-introduced signal features, and technologies that can be deployed at the tactical edge that deliver the capability to the warfighter. Precise Systems' Y-STN signal analysis workflow provides the environment for development and maintenance of the capability, while our INT-PAS technology provides edge-deployment of the capability.

Y-STN IS A COMPLETE RF DATA ANNOTATION, SPECTRUM ANALYSIS, AND ML MODEL TRAINING WORKFLOW THAT IS FULLY COMPATIBLE WITH THE SIGMF STANDARD.

INTELLIGENCE PROCESSING & ANALYSIS SYSTEM **(INT-PAS)** IS A MODULAR EDGE-DEPLOYMENT HOST THAT CAN BE CONFIGURED FOR SINGLE OR MULTIPLE ML MODELS, AND CAN BE INTEGRATED WITH OUR PROPRIETARY INFERENCE ENGINE FOR REAL-TIME SIGNAL ANALYSIS.

MILITARY RELEVANCE

CORE CAPABILITY: The multitude of military applications that emitter fingerprinting enables are predicated around the ability to identify specific emitters in the spectrum, providing the fundamental data from which other capabilities can be realized.

ANTI-FRATRICIDE: The ability to distinguish between Blue and Red Force transmissions and equipment in a congested RF environment provides a separation that enables deconfliction and tracking of all items of interest within the spectrum battlespace, reducing the risk of fratricide and unintended disruption of friendly communications.

BATTLESPACE MANAGEMENT: Tracking specific emitters present in a congested environment, including multiple instances of the same class of emitter provides advantage in maintaining electromagnetic order of battle (EOB). Real-time EOBs with increased accuracy enhance a comprehensive understanding of the battlespace.

MULTIPLE THREAT DISAMBIGUATION: Distinguishing between multiple threats with similar signatures in proximity to one another provides the mission system and operator with greater situational awareness when determining the appropriate counter-action.

COGNITIVE EW: At the edge, real-time identification of a specific emitter provides a system with data to identify, locate, track, and engage. The deployment of trained models at the edge, for example within INT-PAS, provides a capability where an action can be determined and managed within very small timescales.

COUNTER-SPOOFING: Being able to distinguish between source emitter hardware instances provides the capability to determine whether a specific emitter propagated a transmission. This enables a factor of authentication to determine authenticity of a sender, and of RADAR return signals to detect false returns, including signals that have been manipulated through adversary Digital Radio Frequency Memory (DRFM) devices.