

MODULAR ADVANCED CYBER ENABLEMENT SYSTEM (M.A.C.E.)

M.A.C.E. provides practical cyber security training for OT & IT systems by incorporating realistic environments with real-world hardware and technology. The modular design allows for rapid transition between multiple customized training scenarios and environments that can be stand-alone or networked for incorporation into a Cyber Range training program.

► SPECIFICATIONS:

M.A.C.E. leverages Raspberry Pi 3 to minimize the hardware footprint while maintaining peak performance. Our compact design houses a CPU, display screen, sensor modules (E.g., atmosphere or motion sensors), and hardware module for the training scenarios—all in a ruggedized case for storage and transporting. The next-generation design will be moving from Raspberry Pi 3 to later generation Raspberry Pi technologies and NVIDIA Jeston GPUs to increase the processing capabilities and integration of hardware components to expand functionality.

► CUSTOMIZATION:

The M.A.C.E. system's construction allows users to quickly shift plug-and-play components between different scenarios and training plans.

► FUTURE COMPONENTS:

In the current design, multiple scenarios can be stored, but only the runway light model is incorporated out of the box. The next-generation design will allow for additional snap on/off representation models (runway lights, power plant, traffic lights, etc.), enabling multiple models to be used in a single case.



Multiple scenarios and environment models are currently available to train on basic-to-advanced infrastructure systems and critical concepts for defending systems. Request a quote for a custom kit and scenarios to satisfy your individual training needs.

► USE CASES:

Defensive Cyber Operator Training:

The Mobile Advanced Cyber Enablement system provides a flexible and in-depth converged IT & OT training platform. Operators will be introduced to OT protocols, devices, and system configurations, allowing them to begin triaging cyber vulnerabilities and threats within facilities, components, and weapon systems. The M.A.C.E. System incorporates modular system add-ons such as run-way lighting system, manufacturing simulations, power system components and traffic control systems that introduce common use cases of critical infrastructure control systems. Users gain understanding through hands-on experience operating real-world protocols and configurations. Operators also learn how specific TTPs utilized to analyze, hunt, and defend on traditional IT may not be capable of identifying threats or potentially cause harm to the OT systems they are attempting to defend.

Systems Integration Cyber Awareness:

M.A.C.E. gives non-cyber personnel the ability to see real world examples of the implementation of OT protocols and processes, into which they can begin to incorporate and implement security controls and raise awareness to protect against future threats. It provides a platform for integrators, facilities owners/operators, electricians, HVAC technicians, and any other personnel directly involved with designing and operating control systems to gain in-depth knowledge of cyber threats and vulnerabilities targeted by adversaries.