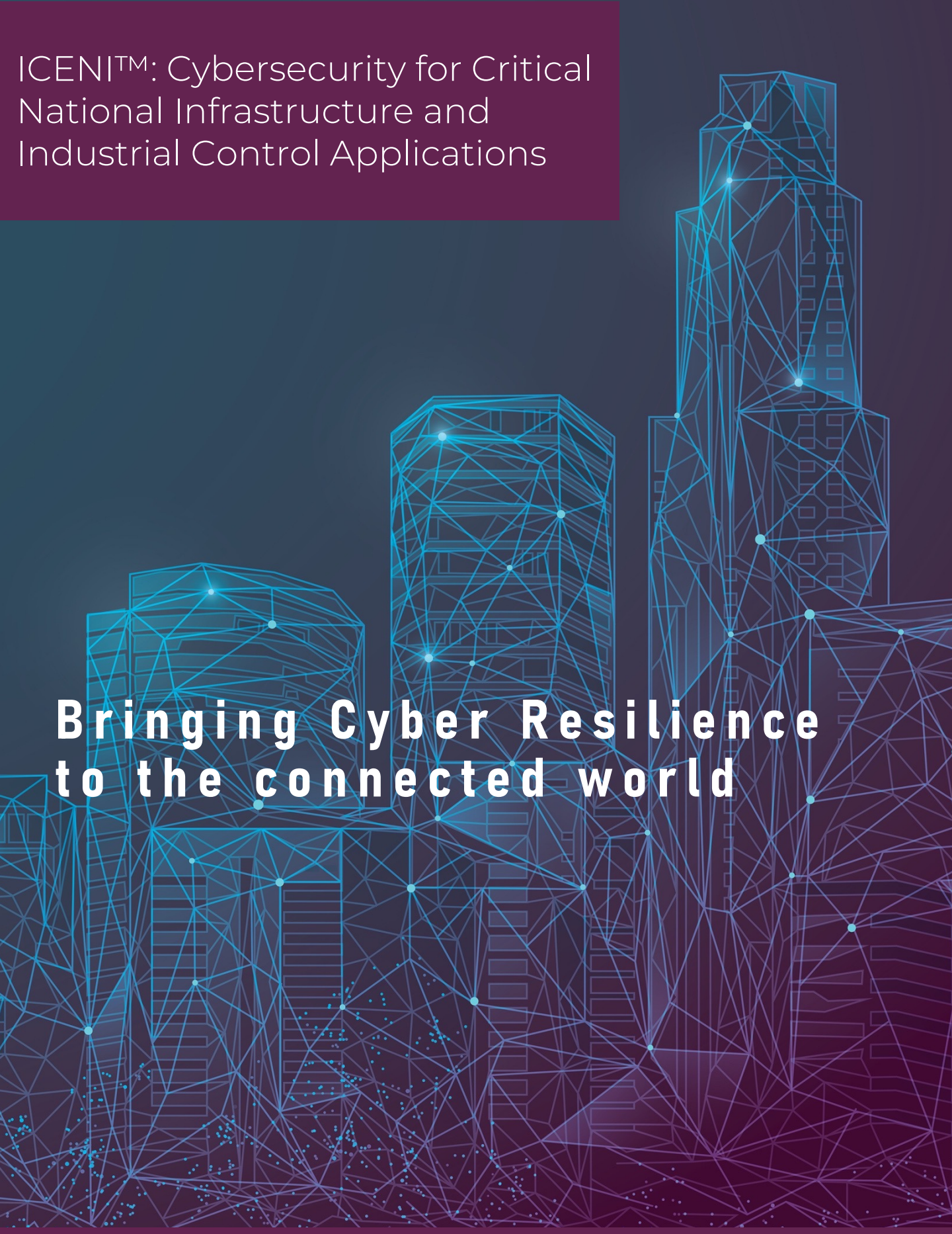
ICENI™: Cybersecurity for Critical National Infrastructure and Industrial Control Applications



Bringing Cyber Resilience to the connected world

Secure. Resilient.
Uncompromising

SCI Semiconductor

ICENI: Bringing Cyber Resilience to the connected world

Memory-safety vulnerabilities account for approximately 70% of all reported security flaws in embedded software. ICENI eliminates this entire class at the hardware level. Built on the CHERIoT capability architecture, ICENI replaces the restricted number of coarse-grained protection regions of a legacy MPU with fine-grained, hardware-enforced memory compartments, with minimal performance overhead. The result is an order-of-magnitude increase in isolation granularity on a single microcontroller.

Summary

Across the use cases described in this document, the underlying pattern is the same: memory-safety flaws provide the dominant path from a network-facing interface to safety-critical control logic. ICENI eliminates that path at the silicon level. Protection is architectural, not dependent on patching cadence or software configuration, and it persists over the full operational lifecycle of the device. For procurement teams evaluating long-lived, mission-critical assets, this represents a structural reduction in risk that software-only mitigations cannot match.

https://www.scisemi.com/company/contact-us/

Secure. Resilient.
Uncompromising

SCI Semiconductor

Making Autonomous Drones Cybersecure

Autonomous drones are uncrewed aerial vehicles (UAVs) that can operate without continuous human control and are designed to perceive the environment using sensors; decide what actions to take based on onboard algorithms; then act by controlling the flight and navigation systems to complete its mission.

Because autonomous drones make decisions onboard, a cyber-attack can influence navigation, targeting, or mission logic without immediate human correction. This increases the potential impact of software vulnerabilities.

Why is cybersecurity important for autonomous drones?

Autonomous drones run complex software stacks, often built on embedded operating systems. Vulnerabilities, especially memory safety flaws, can be exploited to gain control of flight systems, disable safety mechanisms, or install persistent malware.

Key cybersecurity vulnerabilities

- Wireless link exposure: Compromised connectivity allows injection of false commands and degrades availability, particularly when operating beyond line-of-sight.
- GPS spoofing: Navigation and timing rely on unencrypted signals; false inputs can mislead positioning or trigger airspace violations.
- Software supply-chain risk: Update mechanisms and third-party libraries introduce unvetted code paths that an attacker can exploit.
- Shared memory and privileges: Flight control, communications and payload processing often share a single address space, so a fault in one function can compromise the others.

How does memory safety address autonomous drones' vulnerabilities?

Memory safety eliminates a major class of software flaws that attackers exploit to gain control over flight systems, autonomy logic, and communication systems.

Autonomous drones continuously process untrusted inputs from wireless links, GPS signals, cameras, and other sensors. Memory-safe software ensures that malformed or malicious inputs result in controlled failures and recovery rather than silent corruption or attacker-controlled behaviour, reducing the impact of spoofing and injection attacks.

How ICENI enables secure memory for autonomous drones

ICENI provides hardware-enforced memory safety and fine-grained isolation, preventing many of the software vulnerabilities that attackers exploit to compromise flight control, autonomy logic, and communication systems.

CHERI replaces traditional raw pointers with unforgeable, hardware-protected references that precisely define accessible memory region, the bounds of that region, and what operations are permitted. This prevents common embedded-system vulnerabilities such as buffer overflows, out-of-bounds accesses, and use-after-free errors from being exploited to hijack the flight control or autonomy software.

CHERI's support for fine-grained compartmentalisation within a single system allows separation of key functionality, including communication stacks, and algorithms for flight control, autonomy, and navigation.

Secure. Resilient.
Uncompromising

SCI Semiconductor

Resilient Command and Control (C2) Systems

Command and Control (C2) Systems are the mechanisms by which an organisation monitors, directs and coordinates assets and operations, to facilitate situational analysis, decision making and task management across distributed platforms. They aggregate inputs from multiple sources and issue commands to systems in near real time.

In practice, C2 functions are typically hosted on deployable tactical edge servers or mission-planning gateways. These devices aggregate feeds from multiple sensor platforms, fuse situational data and issue tasking commands across distributed units. Their position at the boundary between classified and tactical networks makes them a high-value target for adversaries seeking to degrade operational effectiveness.

In these designs, memory safety flaws can be readily exploited to escalate from localized faults into full control-flow compromise, undermining system integrity, and enabling systemic failure.

Why is cybersecurity important for C2 systems?

Cybersecurity is critically important for C2 systems because these systems function in environments where failure can cause severe physical, economic, or national-security consequences.

Attackers target C2 systems through network interfaces, data feeds and points of integration with other systems. Malformed messages or protocol handling flaws can be triggered remotely, allowing attackers to manipulate decisions, disrupt coordination or gain persistent access.

How does memory safety address C2 system cyber vulnerabilities?

Memory-safety vulnerabilities are particularly acute in C2 architectures because a single exploited flaw can propagate from a compromised data feed into the command-dissemination path, degrading coordination across an entire operational theatre rather than affecting a single platform. ICENI's hardware-enforced compartmentalisation isolates data ingestion, fusion logic and command output so that corruption in one path cannot influence the others.

Memory safety bugs are also notoriously difficult to detect through static analysis, costly to mitigate through runtime checks, and challenging to assess in terms of their downstream impact. As a result, they represent a class of risk that is both high-impact and inherently unpredictable.

How ICENI enables secure memory for C2 systems

CHERI separates data ingestion, decision logic, and command dissemination into distinct compartments.

Hardware-enforced boundaries ensure that memory corruption in one function cannot affect the others. In practice, each major function runs in its own hardware-enforced software compartment, with strictly limited memory access and authority.

Secure. Resilient.
Uncompromising

SCI Semiconductor

Securing Grid Protection

Intelligent Electronic Devices are micro-processor-based components used in power grids to provide protection, control, measurement, and automation functions which include fault detection, circuit breaker operation, and communication with supervisory control and monitoring systems.

They execute deterministic algorithms that decide when to trip breakers, block operations, or change operating modes. Modern devices also provide configuration interfaces, event recording, communications, and remote management to support efficient grid operations.

Their increasing reliance on software and network connectivity exposes them to cybersecurity risks such as unauthorized configuration changes, malicious command injection, denial-of-service attacks, and exploitation of software or memory safety flaws.

Under the EU Cyber Resilience Act and NIS2, grid operators face legal liability for software vulnerabilities in connected devices. ICENI's hardware-enforced compartmentalisation provides a demonstrable, architectural basis for duty-of-care compliance, reducing the burden of evidence required during certification.

Why is cybersecurity important for protecting power grid infrastructure?

Cyber incidents can rapidly manifest as physical outages and equipment damage. If compromised, these systems grant attackers the capacity to manipulate the grid, moving far beyond mere data theft.

How does memory safety address power grid vulnerabilities?

Protection devices process complex protocol messages and configuration data. Memory safety vulnerabilities in message parsing, configuration loaders, or event handling can be triggered remotely. In conventional systems, this can provide code execution inside a device responsible for real time safety decisions. An attacker may aim to disable protection, modify settings, or create timed maloperations during a wider grid disturbance.

Grid systems rely on network-facing software to process protocols used by SCADA substations, and control centres. Memory safety ensures that failures in protocol parsing or message handling results in controlled and managed faults, significantly reducing the risk posed by external or compromised network inputs.

CHERI enables secure memory for power grids

ICENI's implementation of CHERIoT isolates protocol parsing stacks, which are the most frequent point of ingress for grid attacks, into hardware-enforced compartments. A zero-day exploit in an IEC 61850 parser, for example, cannot reach the deterministic trip-logic of the relay because the two functions occupy separate, hardware-bounded memory regions.

Hardware-enforced boundaries ensure that memory corruption in one function cannot affect the others. In practice, each major function runs in its own hardware-enforced software compartment, with strictly limited memory access and authority.

Secure. Resilient.
Uncompromising

SCI Semiconductor

Making Programmable Logic Controllers Cybersecure

Programmable Logic Controllers (PLCs) are rugged, industrial computers designed to automate and control machines and processes in factories, utilities, and critical infrastructure. They continuously monitor inputs (sensors, switches), execute control logic, and update outputs (motors, valves, relays) in real time.

Deterministic timing for predictable control behavior makes PLCs reliable for time-sensitive industrial tasks. Today's PLCs often connect to supervisory systems like SCADA platforms for monitoring and remote control. This connectivity improves efficiency but also increases cybersecurity exposure.

Why is cybersecurity important for PLCs?

PLCs directly control physical industrial processes by issuing real-time commands to motors, valves, pumps, breakers, and actuators. A cyber compromise of a PLC can cause equipment damage, safety incidents, environmental harm, or large-scale service disruption, not just data loss.

As PLCs become more network-connected, they assume trusted networks but they lack strong authentication processes, often using legacy protocols, making them vulnerable to cyber-attacks.

With an operational lifespan of 15 to 30 years, PLCs face a patching deficit in which legacy vulnerabilities remain exploitable for decades. ICENI eliminates the dominant attack vector, memory-safety flaws, at the hardware level, so these cannot be exploited regardless of software patch status. Non-memory-safety issues such as logic errors, authentication weaknesses and configuration drift still require software maintenance, but removing the largest vulnerability class transforms the patching calculus from urgent and reactive to planned and manageable.

How does memory safety address PLCs cyber vulnerabilities?

PLCs directly control physical equipment, hence improving memory safety has immediate safety and reliability benefits. By eliminating a major class of software flaws attackers can no longer manipulate control logic, gain persistent access, or disrupt industrial processes.

PLCs must process untrusted inputs from industrial networks and supervisory systems. Memory-safe designs ensure that malformed or malicious messages are discovered, and are recoverable from, rather than silent corruption or attacker-controlled behaviour. Memory safety contains faults within the affected component, preventing escalation into full device compromise or unsafe control actions, preventing corruption in one software component from spreading across the system

How CHERI enables secure memory for PLCs

CHERI supports multiple compartments within a single device, allowing separation of functions such as communications, control logic, safety interlocks, and diagnostics. A vulnerability in a network-exposed component cannot corrupt or override safety-critical control functions.

PLCs often operate for decades and are difficult to patch frequently. CHERI provides security guarantees that remain effective over the lifetime of the device, reducing reliance on complex software mitigations and ongoing updates.

CHERI strengthens PLC security by moving memory protection from fragile software defences to hardware-enforced capabilities, preventing control-flow hijacking, containing faults, and protecting safety-critical industrial control logic.

Secure. Resilient.
Uncompromising

SCI Semiconductor

Hardened Remote Terminal Units (RTUs)

Remote terminal units sit at the edge of a range of industrial control systems including systems such as energy networks, monitoring and controlling substations, pumping stations, pipelines, and distributed assets. They collect sensor data, control outputs, issue commands, and communicate with supervisory systems.

RTUs are often deployed in remote locations with limited physical security and long maintenance intervals. As utilities modernise, the functionality RTUs provide has diversified to include IP networking, remote configuration, and software updates. These additional connectivity and software elements have increased the attack surface of these devices.

Why is cybersecurity important for RTUs?

Many RTUs use industrial protocols such as Modbus and DNP3 which were designed for trusted, isolated networks and lack authentication, encryption and integrity checking. In a conventional RTU, a vulnerability in the protocol parser shares the same address space as the control logic, so a successful exploit grants the attacker access to actuator commands. ICENI isolates the parser in a hardware-bounded compartment with no capability to write to control-logic memory, limiting the damage even when the parser is fully compromised.

Many RTUs use legacy microcontrollers and embedded stacks that were built for availability and field reliability and not for adversarial exploitation. Memory protection is often limited and coarse-grained with multiple functions sharing one address space for cost reasons. MPU boundaries are insufficient to enforce fine-grained constraints inside parsers handling complex and frequently underspecified protocols.

How does Memory safety address these vulnerabilities?

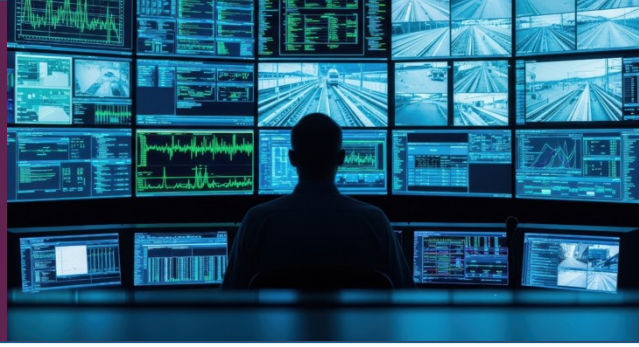
RTUs deployed in remote substations, pumping stations and pipeline junctions present a particular operational challenge: when a memory-corruption exploit causes a system-wide crash, the recovery process requires a physical site visit that may take days to schedule and execute. ICENI's hardware-enforced compartmentalisation confines faults to the affected component, preventing protocol parsing vulnerabilities from cascading into the control and monitoring functions. In practice, this means the RTU continues to perform its core safety role even when a network-facing interface is under attack, reducing both the frequency of unplanned site visits and the window of exposure during which the asset operates without supervision.

How CHERI enables secure memory

In practice, this architecture is realised as a set of hardware-enforced software compartments. Each major function executes within its own compartment, with explicitly bounded memory access and authority.

CHERI capabilities ensure that memory corruption or attempted code execution within one compartment cannot access, modify, or influence the state, memory, or control flow of any other compartment.

Enabling Trusted Train Operations with Cybersecurity Resilience



Modern rail networks depend on software-intensive, always-connected systems to manage train movement, signalling and passenger information.

On-Board Units (OBUs) continuously supervise train speed and braking against movement authorities received from trackside infrastructure, while Automatic Train Operation (ATO) systems automate acceleration, cruising and stopping sequences. As grades of automation increase, so does the software complexity and the corresponding cybersecurity attack surface.

Grades of Automation (GoA) define the level of autonomy of the automatic train operation. As autonomous aspects become more prolific then so do the risks with respect to cybersecurity violations.

Why is cybersecurity important for Trusted Train Operations?

Modern railways are highly connected, software-driven, networked systems. Cyber incidents can directly translate into real-world safety, service, and financial impacts.

If a system is compromised then incorrect speed limits could be sent, braking commands could be delayed or blocked, or trains could stop unexpectedly or fail to stop. Very quickly cyber vulnerabilities can become major safety incidents.

Always-connected trains have a larger attack surface exposing them to remote attacks with a risk of cascading failures across the network, introducing fragility into these smarter railways.

How memory safety address Trusted Train operations cyber vulnerabilities?

Legacy software retrofitted with IP or radio connectivity is especially vulnerable to memory corruption bugs. Memory-safe components act as a containment barrier, limiting how far an attacker can progress even if external interfaces are exposed.

Many train control systems rely on C/C++ for real-time performance. These languages are vulnerable to buffer overflows that can allow attackers to overwrite memory and alter control logic. Memory-safe languages and runtimes prevent out-of-bounds memory access, stopping a large class of remote code execution attacks at their source.

How CHERI enables secure memory for Trusted Train Operations

In safety-certification terms, ICENI provides hardware-enforced Freedom from Interference (FFI). Networking and diagnostic code, which operates at a lower Safety Integrity Level, is physically prevented from writing to memory regions owned by SIL-rated movement-control and braking functions. This separation is maintained by the hardware regardless of software state, simplifying the evidence case for EN 50129 and IEC 61508 certification.

For existing fleets, ICENI can be deployed as a secure edge gateway that wraps legacy C/C++ software in a hardware-enforced sandbox, providing immediate compartmentalisation without requiring a full rewrite of the onboard software stack. For new builds, ICENI serves as the primary processing platform with security designed in from the outset.

Secure. Resilient.
Uncompromising

SCI Semiconductor