SECURITY-FIRST LINUX DISTRIBUTION FOR MISSION-CRITICAL EMBEDDED SYSTEMS

What is TSEL?

TSEL (The Security Enhanced Layer), by 21SoftWare LLC, is a security-hardened, optimized Linux distribution for mission-critical embedded systems. Built on the industry-standard Yocto Project, it implements secure-by-design principles and a zero-trust model to minimize the attack surface, enforce strict perimeter controls, and provide continuous security posture assessment while prioritizing reliability and performance.

Security

Prevent unauthorized access through enforced permissions, strong cryptography, and vulnerability management.

Integrity

Validate and protect the operating stack with verified boot, file-system integrity, and transparency.

Manageability

Safe, reliable OTA updates with automatic recovery keep systems secure throughout their lifecycles.

Key Capabilities

- ✓ A hardened OS foundation tailored for critical embedded systems
- ✓ Secure Boot with a verifiable Chain of Trust (CoT) and integrity protections
- ✓ Policy enforcement with SELinux and an essential-only (default-deny, allowlist) service posture
- ✓ Software Bill of Materials (SBOM) generation in SPDX format
- ✓ Automatic rollback on failure and support for staged flashing and verified reboots
- ✓ CVE Scanning against the National Vulnerability Database to flag vulnerabilities
- ✓ Standards-based security policies with automated configuration baseline validation
- ✓ Minimal network exposure, password hashing, and strong encryption
- ✓ Software Development Kit (SDK) streamlining application and library integration

Proven & Ready

An independent security assessment (December 2025) confirms TSEL is mission-ready. Penetration testing yielded no successful exploits, and the review validated a strong baseline. TSEL blocks spoofed update servers, maintains a single secured access path, protects credentials, and verifies system integrity at boot and during updates. Bottom line: a secure, update-ready operating system engineers can deploy with confidence.

Architecture, Compliance, and Deployment

Architecture at a Glance

- Yocto Scarthgap (LTS) base; builds orchestrated via BitBake 'recipes' for reproducible, configurable images
- Immutable root filesystem secured with dm-verity; detects tampering and prevents booting modified images; supports automatic recovery.
- Mender OTA provides secure, validated image updates with signed artifacts and automatic rollback on failure.
- Platforms: ARM (32/64-bit) and virtual targets; RISC-V is on our roadmap.
- Build and Test Pipelines via GitHub/GitLab

Standards & Zero-Trust Alignment

Aligned mappings available for NIST 800-53/-171 control families, NASA-STD-1006A, FIPS 140-3 crypto modules, CCSDS guidance, and DoD Zero Trust principles. Vulnerability checks against the National Vulnerability Database and policy-based hardening.

Deployment & Operations

- ✓ **Customer Portal** - Access images, release notes, OTA patches, documentation, and build artifacts including SBOM, security/compliance reports and CVE status.
- ✓ **Automated, reproducible builds** - CI/CD-driven Yocto builds with traceable inputs and builds queued via the portal, ensuring consistent images and auditable builds.
- ✓ **OTA Updates** - Stage/flash/verified reboot with automatic rollback; secure, partitioned OTA using a trusted update service.
- ✓ **Continuous monitoring** - Vulnerability scanning and prioritized reporting to keep images current as threats evolve.

Next Steps

- → Scope compliance requirements with our team to map TSEL controls to your standards
- → Request a NASA cFS/COSMOS demo or a short integration assessment on your flight hardware
- → Get in touch with 21SoftWare about how we can otherwise meet your needs: info@21sw.us

21SoftWare LLC secures embedded systems for space and other mission-critical domains. Our flagship product TSEL provides a security-first Linux foundation, and our team brings cyber-security, software, and embedded systems expertise to help customers design, integrate, and operate resilient platforms.