




THE SECURITY ENHANCEMENT LAYER

21SoftWare LLC, has developed an optimized Linux-based operating system for embedded devices that provides a security hardened Linux distribution. TSEL locks down an embedded processor system and provides a protective barrier against attacks while minimizing its footprint on the controller.

TSEL is based on the industry standard Yocto open-source Linux project and supplies features and capabilities that enhance the security and operation of the selected embedded controller. To minimize the attack surface, TSEL implements a zero-trust approach, enables only required features, disables debugging features that can be used in attacks and employs strict firewall and perimeter controls. A key feature of TSEL is the built-in security framework that applies security controls and follows best practices from industry security compliances guidelines to meet your security needs. **21SoftWare** maintains a library of rules from multiple guidelines that are enforced at build time on the images.

TSEL uses several tools to track and evaluate outstanding common vulnerabilities and exposures (CVE) against all software components. Prior to a new TSEL image build, a live check is run for any new notices to ensure known vulnerabilities are addressed.

- 
- ✓ TSEL includes support for Kerberos, IPSec, Wireguard, and DNSSEC and disables weak cryptography.
 - ✓ TSEL uses a signed and hashed root file system with additional storage for audit logs and additional storage through separate partitions.
 - ✓ TSEL supports Secure Boot operations to ensure that software on the device has not been tampered with.
 - ✓ TSEL includes firewall support to enable customers to limit the devices' network communications and meet compliance requirements.
 - ✓ TSEL provides an intrusion detection system (IDS) and auditing and alert features that enable real-time monitoring of threats and unexpected system events.
 - ✓ TSEL includes a list of all the open-source and third-party components, along with dependencies and metadata.

21SoftWare audits each TSEL image when it is built to ensure no unexpected permissions are granted to any binaries on the system that can later be leveraged by an attacker to escalate privileges or access. Standard features include Pluggable Authentication Module (PAM), SELinux, and access control tools as part of every build of TSEL. TSEL supports efficient on-orbit upgrades. A new software image can be staged, flashed, and rebooted on existing spacecraft to bring the system up to date, enabling security, stability, and functionality improvements. Security checks ensure that the new software version is verified and functional. TSEL will automatically revert to the previous image in the event of detected issues.



WWW.21SW.US