aesec™
The power of verifiable protection™

Verifiably Secure PLC on GEMSOS™ Security Kernel

High Assurance Integrity Protection for Cyber-physical Control Systems

Aesec's proof of concept shows the feasibility of using our trusted device to protect a programmable logic controller (PLC) from espionage attacks like Stuxnet and SolarWinds. We implement a PLC on the GEMSOS security kernel, which is designed to meet TCSEC Class A1 certification. This demonstrates that a verifiably secure PLC that could control critical power grid components and their settings while protecting itself against malicious software subversion. This architecture is also transferable to industrial internet of things (IOT) components.

Mitigating Threat of Subversion

The 2020 Presidential Executive Order 13920 on Securing the United States Bulk Power System requires that electric equipment purchased for use in the nation's power grid make provision to defend against the subversive threat to the power grid's safe and secure operation. That is precisely the problem of espionage attacks like Stuxnet and SolarWinds -- they introduce malicious software to subvert the controls a system relies on for its security.

Current PLC and operating systems do not effectively protect themselves against this threat. If malicious software is introduced into the system through supply chain subversion, thumb drives, social engineering or many other techniques, the attacker can take over the PLC. But Aesec's PLC proof of concept demonstrates technology that is in fact distinguished by protecting itself against malicious software subversion.

The U.S. National Institute of Science and Technology (NIST) states for the Electric Grid and the electric utility industry that, "Many commercial products … represent highly trustworthy components and systems that have been verified to be highly resistant to penetration from determined adversaries, and, ***in the case of TCSEC Class A1, distinguished by substantially dealing with the problem of subversion of security mechanisms***"[1] [Emphasis supplied.]

NSA previously evaluated the GEMSOS security kernel and the GEMSOS product Ratings Maintenance Phase (RAMP) plan at TCSEC Class A1 in the Gemini Trusted Network Processor (GTNP™)[2]. This confirmed that GEMSOS verifiably protects systems against subversion from malicious software and provided the rating maintenance plan for rapid evaluable updates.

NSA demonstrated their confidence in the security GEMSOS provides when they deployed their Type 1 Crypto Class A1

[1] https://doi.org/10.6028/NIST.SP.800-160v1; Appendix F

[2] http://www.aesec.com/eval/NCSC-FER-94-008.pdf

BLACKER VPN using the GEMSOS kernel to host the key distribution and access control for the system. Other deployments evidenced similar confidence. UK MOD through ICL as OEM used GEMSOS for their CHOTS Guards. These included interfaces to UK classified cryptographic hardware. The Pentagon used GEMSOS as the front-end communication processor for user access to large IBM mainframes at different security levels in the HSRP program.

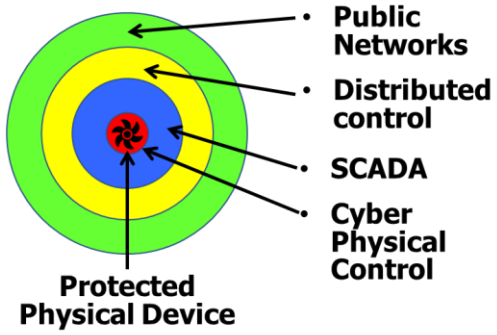
Aesec's proof of concept shows that a PLC can be made verifiably secure using these long-established, effective, inherently secure techniques to substantially mitigate the threat of subversion in cyber-physical control applications.

Designed for System Security

GEMSOS provides system-wide protection because it includes enforcement of mandatory access control (MAC) policies to protect the integrity of the system, and to isolate and protect critical control settings and functions in control applications.

Aesec's innovative approach employs multiple integrity MAC "domains" provided by GEMSOS to dramatically reduce the attack surface available to attackers, as depicted in the following figure:

- **Public Networks** access of any kind gives adversaries a huge attack surface.
- **Distributed control** is vulnerable to insider attack.
- **SCADA** and other adaptable control systems can be sabotaged.
- **Cyber Physical Control** requires the protection of Safe Regions (e.g., Power System Settings) that only Mandatory Access Controls provide. This reduces the attack surface by orders of magnitude compared to any other operating system.



GEMSOS also has the ability to support verifiably secure human to machine interfaces that can be implemented in control room systems for supervisory management.

Commercial Availability

GEMSOS is available under a proven OEM business model. GEMSOS is designed for wide-spread delivery as a Reusable Trusted Device (RTD), providing the security kernel for secure single-board, multi-board, and System-on-a-Chip systems. Aesec provides and supports GEMSOS for specific IA-32 chips to meet original equipment manufacturers and industrial control system integrators needs for their unique hardware. Aesec offers a full Software Development Kit (SDK), open source libraries and a structured operation and developer training course.

For Further Information Contact

Aesec Global Services
info@aesec.com