

Information Security for Land Mobile Radio



NYSTEC is uniquely positioned to help organizations assess and address the security risks to Land Mobile Radio (LMR) systems. NYSTEC has extensive experience with both radio systems and security in information systems. Our combined experience creates a synergy for uncovering the risk to modern radio systems, and employing the best methods for mitigation.

For guidance in assessing threats and vulnerabilities to modern LMR systems, NYSTEC typically characterizes an LMR system as a combination of:

- ▶ **A radio system.** This incorporates the radios and towers and shows risks to items like over-the-air programming features, jamming and physical risks to tower sites.
- ▶ **Voice-Over-IP (VOIP) system.** If the backbone of the LMR is an IP-based network, the system can be susceptible to risks against VOIP, so best practices of securing VOIP must be assured.
- ▶ **Supervisory Control and Data Acquisition (SCADA) system.** Typically, components of an LMR system are unmanned, but require monitoring of components and conditions at remote locations as well as updating the component configurations remotely as required. This places the system in the realm of SCADA and the risk and best practices of securing a SCADA system.

NYSTEC's philosophy is that the biggest challenge to security assurance is how and where to concentrate security assessment activities. To ensure that assessment and mitigation activities are concentrated on areas that pose the greatest risk (threats that have a high chance of occurrence or have a high impact if a threat is realized), the assessment process must begin with a risk analysis. The risk analysis should show:

- ▶ Threats to the components of the system,
- ▶ Likelihood that a threat could be realized, and
- ▶ Estimated cost to the organization or outside entities if a threat is realized.

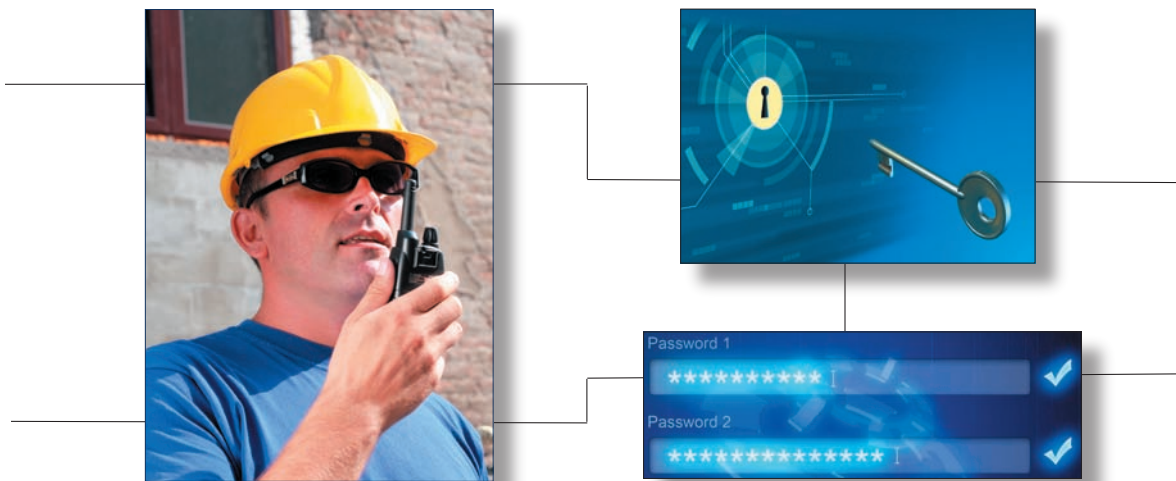


The security assurance of a system must be analyzed throughout the system-development life cycle. Security requirements must be explicitly stated in the system requirements. Threats must be identified and analyzed during system modeling. Actors that may be motivated to manipulate the system to achieve a goal or for personal gain must be discerned.

Security vulnerabilities found in system design and architecture must be corrected before any development or buildout begins. Security tests must be part of the Quality Assurance process in the unit, integration, and final system testing. Finally, operational security processes such as patching, log review, identity and access management must be created and maintained.

When NYSTEC engages in oversight of LMR, we typically review:

- ▶ **Security requirements.** This means ensuring that the requirements speak to mitigating:
 - **Threats to availability.** If the LMR is for emergency response or other life-and-death situations, the top security priority is the availability of the system.
 - **Threats to confidentiality** of the user's voice or data traffic traversing the system as well as system configuration and personal data of users. This review typically involves assessing encryption and access control and how they are used by the system.
 - **Threats to system integrity.** The greatest risks to the integrity of system data are usually those that lead to system downtime (unavailability).
- ▶ **Architecture and design.** Assures that all security requirements are met, and that they are effective in mitigating all risks.
- ▶ **Security testing.** Assurance that the implementation of the system and the procedures are effective in mitigating risks, and that no risks have been left out of the analysis.
- ▶ **Security Policies and Procedures.** The most secure design and system components will not work unless policies and procedures are created to mitigate ongoing residual risks. Auditing measures must also be included to ensure that policies and procedures are enforced.



Bringing Clarity to Complex Technology Projects

NYSTEC
Your Independent Technology Advisor

NYSTEC
www.nystec.com
888-9NYSTEC