## *Attack Methodology Analysis: SQL Injection Attacks*

Database applications have become a core component in control systems and their associated record keeping utilities. Traditional security models attempt to secure systems by isolating core software components and concentrating security efforts against threats specific to those computers or software components. Database security within control systems follows these models by using generally independent systems that rely on one another for proper functionality. The high level of reliance between the two systems creates an expanded threat surface.

To understand the scope of a threat surface, all segments of the control system, with an emphasis on entry points, must be examined. The communication link between data and decision layers is the primary attack surface for SQL injection. This paper facilitates understanding what SQL injection is and why it is a significant threat to control system environments.

Due to the sensitivity of the material, the full text document will only be available to members of the US-CERT secured portal at:

https://portal.us-cert.gov/member/libraryV3/rhsIndex.cfm?action=9&returnAction=32&libid=254796

For additional information on Control Systems, please visit the following site:

***www.us-cert.gov/control_systems***