# Malware Mitigation on RFL Processor Based Devices

Computer malware is a form of software generated by third parties with malicious intent and executed on processor based systems in order to cause undesirable affects. In order for a virus to be written and deployed, the third party must have a deep understanding of the operating system and application software that is targeted. The third party must also have the means to test the virus functionally and finally must have the means to load the virus onto the target device.

In the world of PC's and the internet, viruses (also called malware) are readily created because information on the operating systems and application software is readily available. Hardware to test the malicious software is common (any PC) and methods of deployment (the internet and e-mail) are ubiquitous.

RFL's previous generation products **(IMUX 2000, IMUX4000, 9780/85, 9745, 9300, 9660)** are inherently immune to viruses as they do not utilize conventional operating systems and normally do not have network connections by which malware is distributed. These referenced products do not have security logging or automatically report out SOE events.

RFL believes that while malware can affect any processor based device, it is highly unlikely that third parties would take the time to write viruses specifically targeted at low volume devices with very limited deployment methods. However, because the remote possibility still exists, it is imperative that measures be taken to prevent malware from being installed in customer equipment. RFL relies on the following factors to prevent malware in the GARD 8000.

- Source documentation control – The first step to preventing malware is denying the third party the information needed to write the virus. RFL has in place controls that limit access to the design of the GARD. If the third parties cannot determine how the product operates, it is difficult to write a targeted virus.

- System software control – It is important to make sure the software loaded into the equipment at the factory is not already adversely affected. RFL maintains strict control of its software archiving process and the process by which software is loaded into the product. A change to any software is rigorously tested and then multiple approvals are required before the new software is used in production.

- Network / Password control – The rear port of the GARD 8000 is often connected in some way to a network that exits the substation. It is expected that the utility provides NERC CIP security on this connection, preventing access to the unit. For added security, in the event this is breached, the GARD 8000 provides a multi-tiered access control system that prevents even authorized users without administrator level privileges from accessing important files.

**RFL Electronics Inc.**
353 Powerville Road, Boonton Twp., New Jersey 07005-9151 * USA
Tel: 973-334-3100 * Fax: 973-334-3863 * Web: www.rflelect.com
Electronics Since 1922 * ISO 9001:2000 Registered Company

- Field access limitation – The GARD 8000 web interface does provide access for uploading new files to the unit. This is essential in any powerful unit to provide the flexibility and ease of use required. Application data file uploading can be done through the web server interface using the rear user port and allows the user to load in specific files such as drawings and logic designs to reconfigure the unit. In the event that the network security and password security are both breached files could be loaded into the GARD. During the loading process, the GARD software performs checks to make sure the file meets RFL's requirements. The software of the GARD then uses these files in a specific way as data only and does not ever execute them. While a malicious party with access to this port could download invalid files, there is no way to cause a file to be run as a program, preventing it from acting as a virus.

- Operating system restrictions – As part of the normal software development process, RFL disables many of the features that might allow a user with access to the unit access on the operating system level. These cannot be enabled without physically disassembling the box

- Encryption – The GARD 8000 also supports SSL (Secure Socket Layer) encryption with custom certificates. This feature prevents third parties from listening in to Ethernet traffic and recovering passwords or data.

RFL believes that this combination of procedural controls, security features, and NERC CIP access controls provides a solid barrier against any malicious software.

For further questions or comments, please contact our main office at:

RFL Electronics Inc
353 Powerville Rd
Boonton Twp, NJ, 07005-9151

Phone: (973)334-3100
Fax: (973)334 -3863
Email: sales@rflelect.com
Web: www.rflelect.com