524.

Cyber security

The subject of cyber security has become increasingly prevalent in recent years and NAFLIC has been made aware of a number of examples of attackers targeting a variety of systems and different ranges of equipment and products.

In a report published in Drives & Controls, the global site of the UK's leading magazine for automation, motion engineering and power transmission, one such example NAFLIC was recently made aware of came from the US where cyber security researchers discovered flaws affecting dedicated crypto-authentication chips used in Siemens' S7-1500 family of industrial controllers and related products, which could allow attackers to execute malicious code on these devices.

The report also notes that Siemens has released a list of over 120 products affected by the vulnerabilities and because the defects are associated with the controller hardware, they cannot be corrected by software updates or patches.

Siemens is reported to have stated that because exploiting the vulnerabilities requires physical tampering with the product, it recommends users assess the risk of physical access to their devices and remove any methods of access to devices by outside parties. For example, it suggests placing the affected devices in locked control cabinets.

This is just one example of how controllers and others can be impacted by cyber security related malicious attacks. For those concerned by such matters or those who feel they could be vulnerable to such attacks, NAFLIC would recommend they seek out advice from experts in the field in an effort to avoid future issues. NAFLIC will also continue to monitor areas relating to cyber security and will report of any relevant issues to ensure members remain informed.

Any action advised in the above should be taken to ensure the safety of a device.