Press Release

August 7, 2015

RTP is proud to announce that the RTP3000 TAS is now re-certified to the latest edition of IEC 61508: 2010 Parts 1-7 including its new ATOM^{TM} based Node Processor. The RTP3000 TAS is once again certified to system integrity - SIL-3, the highest integrity level.

RTP has long recognized the importance of the cyber security threat to our customers, and this threat could not be more apparent than the discovery of the Stuxnet virus in a competing PLC product installed at an Iranian nuclear plant.

To ensure that such things are unlikely to happen to our products, we chose to have our product certified in accordance with the stringent ISASecure Embedded Device Security Assurance EDSA-300 by the third-party organization, Exida. The RTP3000 was certified to ISASecure EDSA Level 2 and this certification ensures that it is secure from potential security threat agents and threat scenarios such as malevolent or unauthorized actions. A brief explanation of what is involved follows.

ISASecure certification of embedded devices* has three elements:

- Communication robustness testing (CRT);
- Functional Security Assessment (FSA); and
- Software Development Security Assessment (SDSA).

Specifically, the CRT certifies the capability of the Device Under Test to adequately maintain essential services while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). Testing includes specific tests for susceptibility to known network attacks to identify any vulnerability in networks and devices. You may recognize this test as the Achilles level 1 testing.

The FSA is a rigorous assessment of the security capabilities with the intentions of detecting any implementation errors or omissions.

Finally, the SDSA examines the process under which the product was developed from the point of view of the security of the product.

Next concern RTP wanted to address is how to protect against an unauthorized or unintended access, change or destruction of information between the control system and the host computers and the process of applying security measures to ensure confidentiality, integrity, and availability of data in transit and at rest.

We chose to implement the AES encryption algorithm and this encryption has been added to the communications protocol as the next step in securing the product from cyber attacks. AES is included in the ISO/IEC 18033-3 standard and is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information.

RTP's implementation uses a block size of 128 bits and key length of 256 bits. AES is based on a design principle known as a substitution-permutation network and based on the compute power of the ATOM^{TM} CPU technology has a minimal effort on scan time.

'The addition of the AES encryption to our SIL-3 protocol is yet another example of how RTP listens to our customers' requests for additional functionality" says RTP's President Sal Provanzano

**The RTP3000 Critical Control and Safety System is categorized as an embedded device because it is a special purpose device running embedded software designed to directly monitor, control or actuate an industrial process.*

For more information, visit www.rtpcorp.com