Phone: 1 (877)-825-1530

June 1 2022

FlexSCADA
Mile 2 N Spencer Rd
Lytton BC, V0K1Z0
Canada

RE: Statement of reliability and Security and Recommended Best Practices

Statement of reliability and best practices

FlexSCADA has been manufacturing remote telemetry units for close to 10 years and has built a reputation for reliability and performance under the most demanding conditions from the north pole to the heat of the middle eastern desert.

All of our critical components are supply chain traced and come from North American or European semiconductor manufactures with many of the same ratings you would have in a military, medical, aerospace and automotive fields where safety and reliability is paramount.

While most competitors use systems that operate an entire OS stack which requires regular software patches and updates; we have chosen to engineer our own real-time system from the ground up allowing for several key advantages.

- Longer Product Life Cycle
- Tightened Security
- Lower Power Consumption

Additionally, because of this approach the Q5 needs less than 1MB of memory, so we can use more expensive but much more reliable SRAM type memory which is not susceptible to EMI and Cosmic Rays in the same way that conventional SDRAM or DDR memory is which is utilized by most systems. As an extra layer of protection, the Q5 also adds Error Correcting Codes (ECC) to its memory which is beyond the industry recommendations for SRAM type memory.

Manufactured at our facilities in North America and utilizing a 100% solid state hardware design with no electrolytic capacitors or other elements that rapidly degrade over time we are confident that the Flexs Q5 will provide life long past the warranty period.

Reliability Recommendations and Best Practices

- Ensure devices connected to the expansion port are compatible with the Flexs Q5 and do not have long cable runs (This port is connected directly to the CPU and due to its high speed nature it doesn't have as strong of surge protection as the other ports. (Contact us for design assistance)
- Ensure that the 3.3V and 5.0V ports are safely protected from any cross connections with higher voltage buses or short circuits
- Ensure that proper grounding is setup and that all cables are shielded with proper ESD drains.
- Do not operate the unit where water could splash onto it or where the unit could come into contact with excessive dust or contamination
- For environments where large electrical surges are likely to occur we recommend using an external high wattage burden resistor instead of the internal one for 4-20MA interfacing.

Phone: 1 (877)-825-1530

Statement of security

FlexSCADA takes security very seriously at every level including Hardware Design, Manufacturing and Software Development throughout the entire product lifecycle.

Some of the steps we've made to ensure solid security across our platform are outlined below.

- **Circuit Design and Component Selection**
  - 100% In House design and engineering
  - All key electrical components sourced from reputable North American and European based suppliers including CPU (STMicroelectronics), Ethernet PHY (Texas Instruments), etc.
- **Manufacturing and Testing**
  - 100% In-House manufacturing ensures that only genuine components are utilized during the assembly process and that no backdoors or other hardware modifications are allowed.
- **Firmware and Software Development**
  - 100% In-House software development ensures only our trusted senior software engineers and programmers have access to our codebase.
  - Simplified software development approach
    - Instead of using an entire os stack on our devices like linux which would require regular updates and patches we utilize a bare metal approach including only the code that our software directly utilizes.
    - We believe that well organized, clean and readable code is a foundation for creating a secure platform and have taken pride in our software programming at every level.
  - **Secure Model**
    - Our Flexs Q5 supports industry secure protocols including AES and HTTPS along with the ability to upload custom security certificates.
    - When using the Flexs Q5 with our cloud software (either self hosted or through our services) all communication is encrypted with Pre-Shared-Key AES256 with random cipher block chaining and 256 bit hashing to ensure complete data integrity.
- **Updates and Maintenance**
  - All software updates are encrypted and signed by FlexSCADA and include unique cryptography that ensures only genuine firmwares built by FlexSCADA will run on the FlexSCADA hardware.
  - Updates are usually not required unless new features are added which customers need.
  - Updates are never automatically done and are not a regular part of normal use.
- **Our Guarantee**
  - While nobody can honestly state that their software is and always will be 100% secure we can guarantee that we have done our utmost at every level to create a secure platform and that we have not to the best of our knowledge allowed any weak points or backdoors into our platform at any level.
  - Should a critical vulnerability arise we commit to notifying our customers of the situation and to promptly addressing it.
  - If you have any questions or concerns about the underlying software or hardware we welcome you to contact us.

- **Recommended Security Precautions**
  - **Only load the devices web interface over HTTPS**
    - Without HTTPS all of your web traffic is unencrypted and open for any devices in the middle to view and manipulate. HTTPS adds an additional layer of protection. **Without setting up custom certificates though there is still the potential of a man in the middle style attack. Therefore we recommend either setting up self signed certificates, only accessing the device on the same LAN or using the device on a private secure network (Recommended Option).**
    - Although HTTPS is an industry standard protocol it has a history of falling short due in large part to its extremely complicated design which utilizes hundreds of different ciphers and algorithms. Developers of these ciphers and algorithms have also been caught installing backdoors and loopholes at nation-state levels. Additionally there is the threat of quantum computing and what it could mean in the future to standards that are secure by today's measures.
    - **We therefore recommend that users needing the highest security add an additional layer of protection by only operating the device on a private secure network.**
    - The onboard logic allows users to automate regular functions at remote sites, and **precautions should be taken to ensure that all locally executed code is secure**.
    - **Secure physical access to the device to prevent unauthorized tampering.**
    - Ensure that you only access the device from uncompromised devices. (Many hacks etc are traced back to keystroke loggers, viruses etc that collect personal information without authorization)
    - If an SD card is utilized and the **Device Options->Log Config Changes** option is enabled, the config files saved to the SD card following any configuration changes will contain a hashed version of the password which could be used to access the device if a hacker obtained access to these files. **We therefore recommend that you do not enable this functionality unless you understand the risks associated with it**
- **Technical Information**
  - **Local device password storage**
    - Local devices do not store a plaintext password, instead they store a hashed and salted key (SHA256)
    - Passwords and Device Configurations are stored in the MCU Flash Memory, critical fuses are set to ensure if a hacker has physical access to the hardware that all memory is destroyed if any external read or debugging attempts are made.
    - Firmware is 100% written in ANSI C and executable regions of memory are tightly controlled and protected by a dedicated MPU (Memory Protection Unit) to ensure that no third party code could run alongside our software at any time.