Real-Time Streaming Data Processing Engine for Embedded Systems

K. Tseng, K. S. Yim, Z. T. Kalbarczyk, and R. K. Iyer

Goals

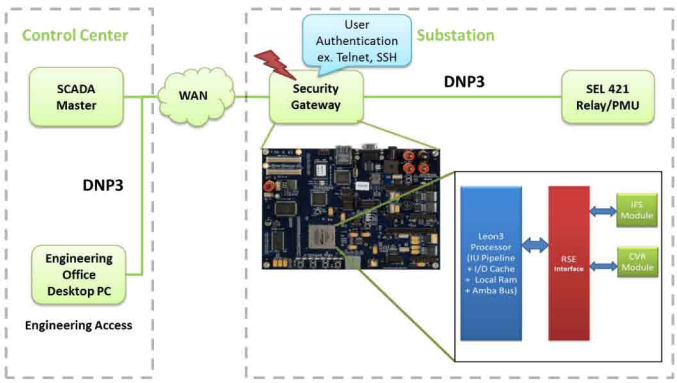
- Develop low-cost, application-specific techniques to achieve secure and reliable execution of applications that compute critical data, in spite of potential hardware and software vulnerabilities.
- Provide flexible and high-coverage method for ensuring reliable and secure computing without incurring much software and hardware overhead.
- In particular, create an embedded device that can be inserted in the Substation Security Gateway to protect data stream against corruption due to accidental errors or malicious attacks.
- In the future, the techniques can be integrated into the chip itself (e.g., a dedicated core).

Fundamental Questions/Challenges

- How to protect critical power grid data from malicious tampering and unexpected errors.
- How to detect application-level internal and external attacks.
- How to provide a standard interface between the Substation Security Gateway and hardware modules that implement reliability and security services.
- How to achieve low-cost, low-overhead, high-performance, and scalable security and reliability checking.

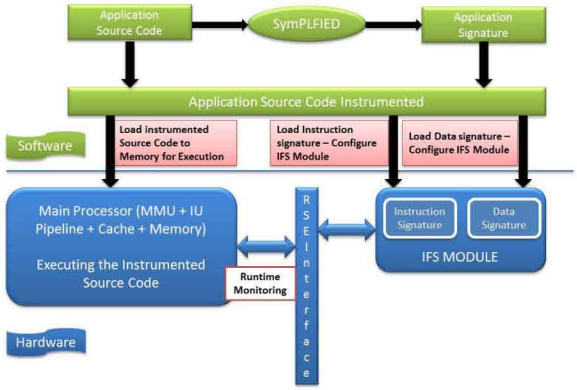
Research Plan

- Apply the Assured Streaming Data Processing Engine on the Substation Security Gateway to provide security and reliability.
  - **Information Flow Signature (IFS):** Analysis of the program to derive the instruction backward slice that manipulates the critical data and to instrument it with code to ensure that runtime modifications of the critical data follow the language-level semantics of the application.
  - **Critical Value Re-computation (CVR):** The application source code is statically analyzed to extract the backward slice for the critical data and then instrumented with the check instructions to recompute critical values.



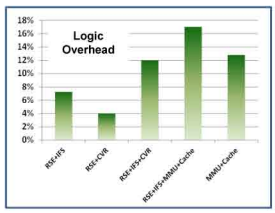
Design & Integration of IFS

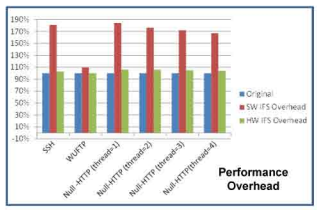
(Information Flow Signature)



Research Results

- Leon 3 processor, RSE framework, and IFS module synthesized to Altera Startix II FPGA.
- IFS module demonstrated using SSH, WuFTP, and NullHTTP applications on top of Linux OS with low performance overhead (3–4%) and 100% coverage for insider attacks.





Broader Impact

- The Assured Streaming Data Processing Engine can not only be used on the Substation Security Gateway, but also on every device that stores critical power grid data to protect its security and reliability.

Interaction with Other Projects

- We utilize the methods and tools developed by the project "Testbed-Driven Assessment" to set up our experimental environment.

Future Efforts

- Combine our working prototype into the testbed set up by the project "Testbed-Driven Assessment," to explore more attack scenarios in real cases.
- Explore the vulnerability of the communication between SCADA and the Substation Security Gateway.