

Nallatech Designs Reconfigurable Video Encryption System for the UK Ministry of Defence with Simulink®

For the military, replacing obsolete components is a costly undertaking that requires a reverification of the entire system. The United Kingdom Ministry of Defence (MOD) contracted Nallatech, a provider of high-performance FPGA systems, to devise a more cost-effective method for managing hardware obsolescence.

Using Simulink® and Xilinx System Generator for DSP, Nallatech designed a reconfigurable video encryption system that enables the MOD to reverify the entire system by updating components, customizing interfaces to those components, and performing validation at a subsystem level—without any knowledge of VHDL.

“Many of our customers do not have any experience with VHDL,” says Malachy Devlin, chief technology officer at Nallatech. “Simulink is the first tool to get us out to the FPGAs without learning VHDL. There really isn’t any other tool that is so comprehensive.”

THE CHALLENGE

Using FPGAs, Nallatech sought to design a reconfigurable system that would prove how the MOD could replace one or more components without affecting the rest of the system and software.

To prove their concept, Nallatech would need to develop an application suitable for military purposes. To demonstrate configurability, they would need to create two versions of the system—one based on an existing system, the other on a more advanced algorithm.

“We wanted to show the MOD how easy it would be to create a new system by dropping a new IP into an existing system,” says Daniel Denning, a research engineer at Nallatech.



Reconfigurable video encryption system.

Nallatech would also need to show that the system could be developed rapidly, without involving any VHDL training and using readily available boards and components.

THE SOLUTION

Using MathWorks tools, Nallatech engineers designed a reconfigurable video encryption system by creating two identical designs with different encryption cores. They completed the project in just two weeks.

For the first encryption core, Nallatech chose a modified Enigma algorithm that was used by German military and intelligence communications during World War II. For the second core, they chose the Advanced Encryption System (AES) algorithm. This widely used algorithm can process data blocks of 128 bits and is known for its parallel structure.

After creating the algorithms, the engineers debugged and integrated the core, formatted the video, and generated the VHDL for the FPGA.

Using an iterative design process based on Simulink hierarchical models, Nallatech

THE CHALLENGE

To design a reconfigurable video encryption system

THE SOLUTION

Use Simulink and Xilinx System Generator for DSP to create algorithms represented in subsystems, debug and integrate the core, format the video, and generate VHDL code for the FPGA

THE RESULTS

- Design time reduced by 2/3
- VHDL training avoided
- Collaborative development accomplished remotely



“ We could not have implemented the algorithms on the FPGA this quickly without Simulink and Xilinx System Generator. ”

—Malachy Devlin, Nallatech

engineers divided up the system tasks. Denning used Xilinx System Generator for DSP blocks within Simulink to develop subsystems of the encryption core within the AES algorithm. He then validated the AES algorithm with publicly available test vectors provided by the National Institute of Standards and Technology.

With Simulink, Denning set the parameter values within the encryption to enable easy modification at the subsystem level. The values were stored in the MATLAB® workspace and then propagated to the models.

Denning used visualization blocks in Simulink to debug the core, using one part of the system as a test harness and another part to isolate defaults. He validated signals, including the video and encryption signals, by comparing live signals with simulated signals represented in subsystems.

Denning's colleague, Neil Harold, placed the encryption core blocks into his Simulink model and integrated them with the top-level system before formatting the video.

“It was very easy to communicate our design using Simulink,” says Denning. “It was also much quicker to produce the cores and check how everything worked visually rather than in VHDL.”

With Xilinx System Generator for DSP, Denning then generated the VHDL to get the bitstream for the Xilinx Virtex-II FPGA.

Using Nallatech's Xtreme DSP Kit, Denning then mapped the system to the FPGA on a BenADDA module, housed on a BenONE motherboard. Video was transmitted over an analog-to-digital wireless link and fed back into the same FPGA for decryption.

Impressed with the results of this project, the MOD is actively exploring ways to adopt this approach for future systems design.

THE RESULTS

- **Design time reduced by 2/3.** “With this design flow, we efficiently implemented our system and algorithms with a significant improvement on traditional design times, without sacrificing performance,” says Denning. “Coding in VHDL would have taken us three times as long.”
- **VHDL training avoided.** Nallatech engineers developed the encryption core without writing a single line of VHDL code. “I didn't have any formalized training in Simulink, yet I could basically draw the circuit and flow it to the FPGA,” says Denning.
- **Collaborative development accomplished remotely.** Using the external mode feature of Simulink, Denning shared models with Harold, who was 600 miles away in another office.

To learn more about Nallatech, visit www.nallatech.com

APPLICATION AREAS

- Algorithm development
- Communications
- Digital signal processing
- Model-Based Design
- Modeling and simulation

PRODUCTS USED

- MATLAB
- Simulink

www.mathworks.com