# A Pilot Course in Vital Electronics

Jerry Gulley[1], Friedrich Holl[2], Ted Kochanski[3], and Andrzej Rucinski[4]

1. Strategic Security Alliance, U.S.A
2. Fachhochschule Brandenburg. Germany
3. IEEE Boston Section, U.S.A.
4. University of New Hampshire, U.S.A

andrzej.rucinski@unh.edu

## Abstract

**Vital Electronics, Testbench, Innovation**

This paper describes the paradigm of "Vital Electronics" (defined in the text) and an associated pilot course. Vital electronics is the response to the challenges of the "post VLSI era," to restore the enthusiasm and interest of students in microelectronics systems. This approach can be integrated within I-GEMS [1], an IEEE-sponsored Global Design Environment, for reliable nano to global scale Critical Embedded Systems.

## 1. Vital Electronics

**Vital Electronics** is the study and use of electrical components, circuits, networks, and systems to achieve a design goal of protecting, saving, and improving critical infrastructure, and hence the quality of life. Vital Electronics' domain is a heterogeneous computing environment derived from sensors networks, embedded systems, and ambient intelligence with intelligent, robust, and trustworthy nodes capable of building **Application-Centric Embedded Computers** from "off-the-shelf" virtual computational and networking parts.

Vital Electronics makes Embedded Computers more capable, reliable, energy-efficient, and optimized to their tasks. These Embedded Computer inhabit our critical infrastructure and other key applications, at increasingly low-levels, and with increasing interconnectedness with their peers. At the same time, Vital Electronics enhance the ease, and speed of the design of reliable Embedded Computers, and their associated Embedded Systems through the reuse of proven and certified "design elements," and other "virtual components."

Vital Electronics is founded on the synergistic interaction between Moore's Law, Metcalf's Law, High-Level System Design Tools and MEMS Sensors and Actuators. The increasingly capable Programmable Systems on a Chip (PSoC) such as Cypress Semiconductor's PSOC family with its companion PSoC Creator tools are the key building blocks of Vital Electronics

## 2. Course Description

Our initial planning assumed two courses in Globally Integrated Security Environment (GISE), run simultaneously, one in the United States and another in Germany [2]. To reduce complexity, logistics, and distance learning challenges, it was decided to focus the Pilot Course on Vital Electronics, as the cornerstone technology segment of GISE.

The course was organized around a hands-on introduction to one such family of PSOCs developed by Cypress Semiconductor, which enables implementing reliable, low-power wireless complex sensor-centric systems incorporating up to 250 nodes. The focus was on a hands-on background in Cypress PSoC®-based Embedded Wired and Low-power, long-duration Wireless Sensor Networks. Attendees were introduced to a wide range of applications including: Home / Building Automation (Smart Grid and Security); Human Input (Cap and Touch Sensing); Medical Devices and Well-Being Equipment; Industrial Process Monitoring and Control; Security, Structural Monitoring; Sports and Leisure; Asset Management, Robotics, Public Transportation.

Cypress PSoC® devices feature: an FPGA-like programmable interconnect fabric, configurable analog and digital blocks, 8 or 32 bit CPUs, Flash program memory, SRAM data memory, and configurable I/O integrated into a variety of compact packages.

This architecture allows the user to rapidly create systems, replacing multiple traditional MCU-based components, with one, low-cost single-chip programmable PSoC device. The Cypress CyFi™ low-power physically compact Direct Sequence Spread Spectrum (DSSS) transceiver, and the logically simple, small-memory footprint lightweight wireless network protocol stack, enables one to build wireless sensor networks incorporating up to 250 nodes to be designed using “drag-and-drop” tools.

## 3. Security Application-Centric Projects

There were three student projects in the pilot course. One of them was the Generic Critical Infrastructure Protection project led by Harry Charache, a student with a security, but not engineering background. The student has designed and built a sensor network called GNAT in the Critical Infrastructure Dependability Lab (CIDLab) at the University of New Hampshire as shown in Figures 1 and 2

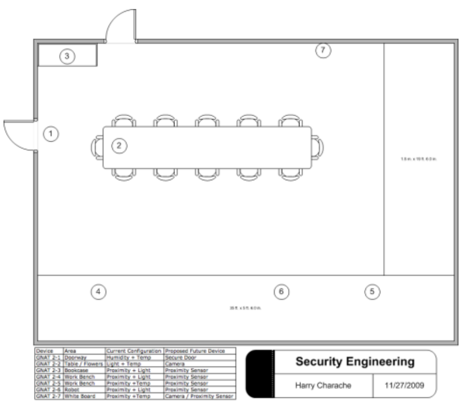


Fig. 1. The placement of GNAT2 sensor nodes in CIDLab.

Fig.2 General view of CIDLab with sensors hidden.

A series of experiments and measurements where conducted to characterize the behavior of GNAT2 computer in case of anomalies e.g. personal intrusion to the lab. The other two pilot projects included Invisible fence: Deployable Proximity Alert System (developed by former US Marine combat veteran Steve Doran) – Figure 3 shows it detecting an approaching vehicle, and Grid security, an energy grid remote monitoring system (developed by working power systems engineer Doug MacMillian).

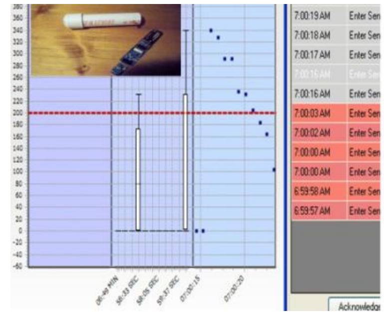

Fig.3.DPAS (inset) and detection of approaching vehicle measures the light change in CIDLab.

## 4. Summary and Assessment

All students have been very enthusiastic about the course and want to continue the effort the next semester. We plan to offer the course again in cooperation with our German partners. We also plan to offer the reduced version of the course for practicing engineers through the IEEE Boston Section short Course and Lecture Series continuing education program, as well as via a course introducing Vital Electronics for non-engineers. The first project is being continued as a master thesis. The third project should lead to a smart grid remote monitoring industrial application. On a negative side, despite outstanding support from Cypress, the laboratories should be reworked and enhanced to speed up the necessary learning curve.

## Acknowledgement

The authors would like to thank Cypress Semiconductors for their generous support of the vital electronics program and specifically to TJ Rodgers, CEO, Patrick Kane, University Program Manager, and Professor Alex Doboli SUNY Stony Brook.

## References

[1] T. Kochanski and A. Rucinski, invited paper, “I-GEMS and Global Security,” 1st International Conference on Information Technology (IT 2008), May, 2008, Gdansk University of Technology, Gdansk, Poland

[2] K. Mikelinich, A. Drozd, L. Izraylo, L. Long, T. Kochanski, and A. Rucinski, Globalization for Design: A Market for a CMP/IP Repository, *EWME2008*, Budapest, June 2008