Sept 87

System Design for a Remote-Access Panel Prototype

M. Pihlman and D. Edmunds

The upcoming automation of the Lawrence Livermore National Laboratory (LLNL) security system under the aegis of the Safeguards and Security Enhancements-Phase 1 program (SSE-1) requires the development of an intelligent, user-friendly communications link between employees and SSE-1's computers. When in place, this remote-access panel (RAP) will be the primary interface between LLNL employees requesting entry through CAIN II booths and access to the SILAS (Secure Interactive Livermore Alarm Station) security systems.

Working in conjunction with the main SSE-1 computers, the RAP will automatically read an employee's badge number for identification and a memorized personal identification number for verification, and, as needed, will receive and transmit biometric information from a fingerprint or retinal scan.

The authors discuss the design of the RAP *prototype,* which was completed in November 1986. *The final designs of CAIN II, SILAS, and the RAP, however, as they are ultimately implemented throughout the Laboratory in the spring of 1988, may differ.*

Introduction

As a result of new standards for security and safety set up by the U.S. Department of Energy, a major upgrade of security systems at Lawrence Livermore National Laboratory (LLNL) is now in progress (see box). This upgrade is in the form of two integrated Congressional line items totaling $61.6 million, the first of which is Safeguards and Security Enhancements-Phase 1 (SSE-1). This five-year project, which commenced in FY 1985, has as one of its two major objectives replacing or upgrading obsolete and personnel-intensive security equipment and systems. This objective has been refined into five technical and three construction projects. The technical projects are to:

- Replace the alarm systems at both Livermore and Site 300 with a new computer-based alarm system, SILAS (Secure Interactive Livermore Alarm System).
- Automate LLNL's access-control system with a redesigned and expanded CAIN (Controlled Access by Individual Number) entry-control system, called CAIN II.
- Restructure security command and control by the integration of all critical realtime functions into a modern, computer-aided console.
- Upgrade the security radio communication network at Livermore and Site 300 with expanded coverage, encrypted transmissions, backup transmitters, and a microwave link between the two sites.
- Modernize the LLNL accountability system for special nuclear materials.

The first two projects concern us in this paper. CAIN II, which will replace the existing TV booths and CAIN booths,* will probably be the most visible of all SSE-1 projects to the LLNL population, as most Laboratory employees will use at least one of CAIN's automated entry-control and passage-monitoring devices on a daily basis. These new automated controlled-entry booths will require an employee to request entry by inserting his or her badge into a badge reader and entering a personal identification number (PIN) on a keypad, in much the way a request for money is made from an automated teller machine. This badge reader and its keypad, LCD, and function switches form a unit known as a remote-access panel (RAP); the interface between the RAP and the automated Security Console will be CAIN II, the new, "smart" entry-control system.

A RAP will also sit outside of each alarmed location, where it will permit authorized personnel to place the alarm station in access or secure

* The TV booths are known by the Laboratory population as "CAIN booths" though no individual number is in fact entered. Real CAIN booths have, however, been in use to separate limited and exclusion areas.

Security at the Lawrence Livermore National Laboratory.

In 1952 the Atomic Energy Commission created the Livermore branch of the University of California Radiation Laboratory to meet the need for a second weapons-design laboratory (a need argued successfully by nuclear physicist Edward Teller and Laboratory Director Ernest O. Lawrence). The Livermore branch employed just 90 people to start. Security consisted of wooden fences on the north and south perimeters, and the Laboratory's few guards—borrowed from neighboring California Research and Development—checked the contents of lunch pails and briefcases as employees entered and left buildings. The new laboratory had no computers, no clearance process, and no document control procedure; there was just a crude badge system.

A few months after its inception, Livermore hired Robert Becker, formerly an FBI agent, to work three jobs: security, safety, and plant engineering. He set up the Security Office and hired three police officers from the Berkeley branch to help organize and supervise a small guard force. The procedures Becker set up were informal, but they worked effectively because of the small size of the Laboratory and the concern and awareness of Laboratory staff.

In the summer of 1954 California Research and Development handed over full control of the old Naval Air Station to the Laboratory, which had up until now occupied only the western one third of the base. The Laboratory expanded the Security Office into the Security Department, which was located in Building 415, but the security staff remained small and still lacked a computerized command control center.

The Laboratory expanded rapidly in the following years. Its first computer began servicing programmatic needs in 1953, and by the next year the number of employees had swelled to 2000. In 1957 the first two programs outside of nuclear weapons and controlled thermonuclear reactions began, Pluto and Plowshare. In 1963, the biomedical program was established, and special building projects were under way to house such items as uranium, plutonium, and tritium. By this time the Laboratory was employing nearly 5000 people, and it was in this year that the Security Alarm Control Console was implemented. In 1976 the Console was moved to its present location in the basement of Building 271, where it continues to operate to this day.

At the present time, the Security Console resides in a small, windowless, poorly ventilated room. Although each piece of equipment was originally added to enhance operations, the long-term result has been a cluttered collection of wires, panels, and video-display terminals. The PFOs squeezed into this room must quickly and accurately examine the faces and badges of impatient employees as they enter through some 100 TV booths.

In the early 1980s the U.S. Department of Energy decided to counteract the rising threat of terrorism with more stringent standards for physical security at its research facilities. Since that time, DOE laboratories engaged in nuclear and other classified research have faced great increases in the requirements for safeguarding information and material. As a result of these new standards, a major upgrade of security systems at Livermore is now in progress, in the form of two integrated Congressional line items totaling $61.6 million. The first line item, called SSE-1 (Safeguards and Security Enhancements-Phase 1), is a five-year project that started in FY 1985, and has two major objectives: to replace or upgrade obsolete and personnel-intensive security equipment and systems, and to construct facilities to house these new security systems. SSE-2 is also a five-year project that started in FY 1987, with the objectives of consolidating and protecting operations with special nuclear materials in a protected area called the Superblock, and increasing the overall protection at LLNL by improving the labwide physical security system.

Two of the SSE-1 projects are to replace the existing LLNL alarm systems with a new computer-based alarm system called SILAS (Secure Interactive Livermore Alarm System), and to automate LLNL's existing access-control system with a redesigned and expanded CAIN (Controlled Access by Individual Number) entry-control-based system, called CAIN II. The primary interface that Laboratory workers will have with these new systems will be the remote-access panel (RAP) at all alarm stations and within the new booths.

mode (among other functions). The interface between these RAPs and the automated Security Console will be SILAS, the new, automated computer-based alarm system.

This paper will discuss the design of the RAP *prototype*, which was completed in November of 1986. *The final designs of CAIN II, SILAS, and the RAP, as they are ultimately implemented throughout the Laboratory in the spring of 1988, may differ.*

SILAS: The existing physical security system, the Security Alarm Control Console, was conceived many years ago for the Livermore site when the Laboratory was smaller and its security needs less demanding (see box). The alarm system at Site 300 is also many years old. Both systems, which, between them, monitor approximately 300 secured areas (consisting of vaults or rooms monitored by magnetic door switches, glass breakage sensors, and infrared sensors) have grown more and more expensive and difficult to operate as the number of stations has increased and the security requirements have tightened. The new system, SILAS, will be required to provide a high level of security, a high level of interaction with security administrators, station users, and system maintainers, and a high level of automation. It is expected that SILAS will initially alarm over 300 secure areas, with possible expansion to 1000.

Alarm stations will be monitored by a microprocessor-based controller—an RTU (remote terminal unit)—which will in turn be connected to a central computer system, the SILAS host, located in an expanded Bldg. 271. This central computer will analyze the sensor and RAP data sent over encrypted communication lines, and take appropriate action such as sounding an alarm if a breach has occurred, or approving entry to a secured area by an authorized person.

CAIN II: The existing TV booths have two TV cameras, one looking at the booth to detect the presence of more than one person, and the other, using a split screen, to look at both the person using the booth and the badge that the user has placed against a small window. Identification is made by a PFO (Protective Force Officer) in Bldg. 271 by comparing the photograph on the badge to the image of the person requesting access. The existing CAIN booths located in exclusion areas require insertion of the employee's badge to initiate access authorization by a central computer. CAIN II booths will automate all entry procedures. The user will interact with the system by means of a RAP device.

The RAP: The remote-access panel (Fig. 1) will be the primary interface between LLNL employees and the CAIN II and SILAS security systems. Working in conjunction with the main security computers, the RAP will read an employee's badge number for identification and a memorized personal identification number for verification; as needed, it will receive and transmit biometric information from a fingerprint or retinal scan.

RAP System Criteria

When implemented, the RAP will allow or deny entry in over 300 SILAS locations and as many as 100 CAIN II locations, requiring daily usage by almost everyone working at LLNL. With this in mind, we developed the following design criteria:

The RAP must meet Security's requirements and be:

- User-friendly
- Attractive
- Reliable
- Easy to maintain
- Able to operate at low power
- Flexible enough to meet any new requirements that develop.

We also needed to assess what subsystems were required to meet these criteria, and if any of these were available commercially. We developed design criteria from these requirements, which are listed below.

Functionality: We envisioned the RAP to work something like this: An employee wishing to enter a limited area could do so through a CAIN II booth. Once inside, the person would read "PLEASE INSERT YOUR BADGE" on the LCD. Once the badge is inserted, the LCD would read "PLEASE ENTER YOUR PIN." If the wrong PIN is entered, the RAP would grant the user two more tries. Once the correct PIN and badge number had been presented, the display would read "PLEASE ENTER TO THE RIGHT. THANK YOU." To do this, the RAP must be able to read a magnetic-stripped badge, accept PIN input, prompt the user during operation, and it must have function keys to assist in usage.

The RAP when used in alarm stations could perform many additional functions, such as telling a maintenance person which sensor is malfunctioning and what condition it's in, allowing a user to be enrolled or disenrolled, allowing a PIN to be changed, and other administrative functions. A HELP option would be available in case of trouble.

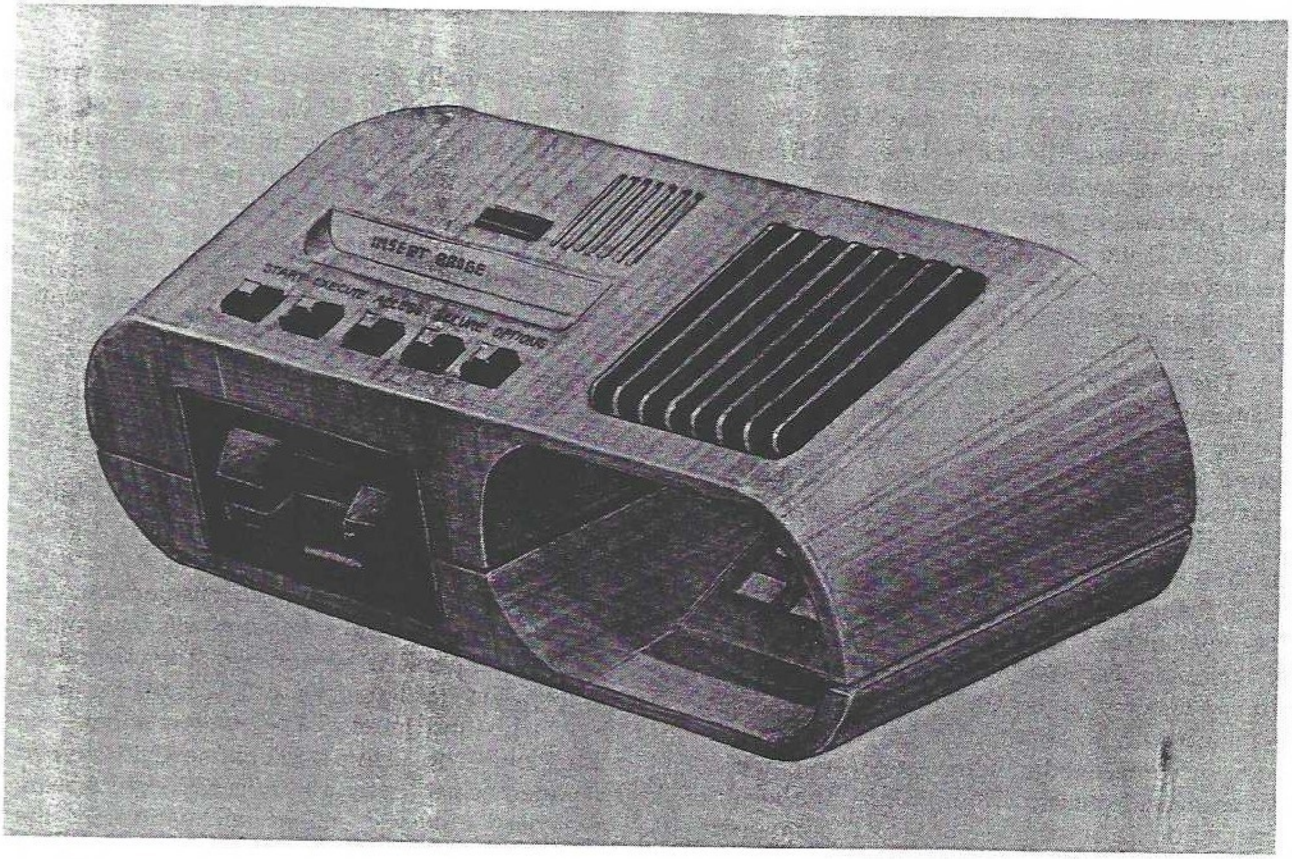


Figure 1. Remote-access panel prototype.

Reliability and Maintenance: Since there will be over 300 SILAS alarm stations and nearly 100 CAIN II locations, a major goal was to design the RAP to be reliable and easy to maintain. The hardware needed to be easy to repair and contain as few components as possible to do the task. We wanted to design the package to be easily replaced in the field and transported for repair. Once in the shop, specially designed automated test equipment will be used to facilitate repair.

The software must be robust and fault tolerant. It must incorporate detailed error-checking routines for messages to and from the host processor, complete subsystem checks, and internal diagnostics. A watchdog timer was required to reset the processor in case an error does occur.

Human Factors: Human-factors considerations for any device are generally left until the end of the design cycle, but since the RAP faces such a demanding user interface, we felt that our human–factors design criteria (ease-of-use and attractiveness) were as important as any other. We wanted attractive packaging, and we wanted to lay out the subsystems in such a way as to create a logical progression of functions.

We needed to select a keypad and decide on a badge-reader type (insertion or swipe).

The RAP must be easy to use for everyone; it must be located on the wall in such a way that it could be used by anyone regardless of height. It must be designed to be sensitive to the needs of the physically handicapped and the visually impaired.

Power Consumption: The 300 or so SILAS alarm stations will be powered by batteries, which will be automatically recharged, so low-power operation was needed to conserve the batteries.

Security: SSE-1 required us to hide the keypad from view as much as possible, to prevent an observer from watching the entry of a user's PIN. The PIN must also be protected over the communication lines to the host processor.

RAP System Design

Because SILAS was evolving as we embarked upon the RAP design, a critical system-design decision had to be made concerning the way the

RAP would operate; that is, we had to make the RAP as flexible as possible in order to meet as yet unspecified SILAS requirements. We did not want to hinder the development of the RTU. This flexibility is embodied by the fact that, with a standard protocol, all functions of the RAP are completely defined by the RTU: The letters displayed on the LCD are sent from the RTU, the buttons pushed on the RAP are answered by the RTU, and the badges are read when the RTU instructs the RAP to read them.

The RAP's 80C31 microcontroller acts as a coordinator assuring that all the devices work together and that any input information is transferred to the RTU in a timely and efficient manner. This flexibility came in handy early on when the CAIN II project decided to use the RAP in their system; with minor hardware and software changes we were easily able to satisfy the requirements of both CAIN II and SILAS.

Human Factors: As mentioned, we placed human factors high on our priority list. To help us come up with an attractive, highly functional design, we contacted the human-factors engineers of the Systems Research Group (SRG). The result of their effort is shown in Fig. 1. All components are mounted in a tamper-resistant polycarbonate housing.

System Architecture: Figure 2 shows the architecture of the RAP controller mother board as designed for the prototype. We designed the board using CMOS devices and included software-controlled power application to the badge reader, which is not power conservative. This makes it possible for the microcontroller to power down the badge reader as required.

The blocks labeled *RS-232, RS-485, Memory, UART,* and *Power* are part of the 80C31-based microcontroller board that we designed to control the other blocks, namely, the badge reader, LCD, keypads, and function switches.

The badge reader is a commercially available magnetic-stripped badge reader chosen by the CAIN II New Badge Committee. This device is a full-insertion, high-coercivity (4000-Oe), 2-track, magnetic-strip reader. It was selected by the committee because of the badge's unique track-0 manufacturing method that makes it virtually impossible to copy or alter if the badge is lost.

The liquid crystal display we originally worked with was a 2-row by 24-character module with 0.5-in.-high characters; but when the housing was designed and we had had some experience fitting prompts on the display, we switched to a 4-row by 20-character display. (The original display is pictured in Fig. 1.)

We originally considered two different types of keypads, and the RAP was designed to use either one. One was an electronic keypad, which has LED numbers that can be electronically scrambled. The keypad numbers were protected by internal sight-screen baffles that inhibit viewing of the numbers further than ±4° horizontally and ±40° vertically, meaning that a casual observer would have to look directly over a user's shoulder to see him/her enter his/her PIN. This was an impressive option for security purposes, but expensive, raising the cost of each RAP by nearly $300.

Eventually, cost and questions of reliability and maintenance forced us to drop this option and pursue a design with a telephone-style keypad. In doing this, power consumption was dramatically lowered, reliability was improved, and the cost per RAP went down. The telephone-style keypad has letters as well as digits for those users who find letters easier to remember. The disadvantage to using a telephone-style keypad was the need to design an effective sight screen. We looked at many options, and ultimately, the SRG Group came up with the solution as seen in Fig. 1. As you can see, the keypad is very effectively hidden from observation by anyone but the user.

Our prototype design includes a beep sequence and keypads with ergonomic spacing and bumps to assist in PIN entry for the visually impaired.

The function switches are momentary push buttons with one LED; these switches may be used to assist with a prompt or used as a "soft" label for a key. For example, the RAP could tell the user to "PRESS THE LIGHTED BUTTON TO ENTER." The function push button and the keypad were chosen for their long life expectancy (>5 million operations) as well as their LED operation and appearance.

One critical function that is not depicted in Fig. 2 but is absolutely essential to the RAP is a DIP switch that tells the 80C31 microcontroller several things upon power-up: whether it is a CAIN II or SILAS RAP, whether or not it has a biometric device, if it should run the diagnostics package, and what its SILAS multidrop address is.

External to the board is either the SILAS remote terminal unit or the CAIN II entry-control device (ECD), which are the processors that control the RAP and communicate with the host processors; see also Figs. 3 and 4. Also external to the board is a biometric device that will be either a

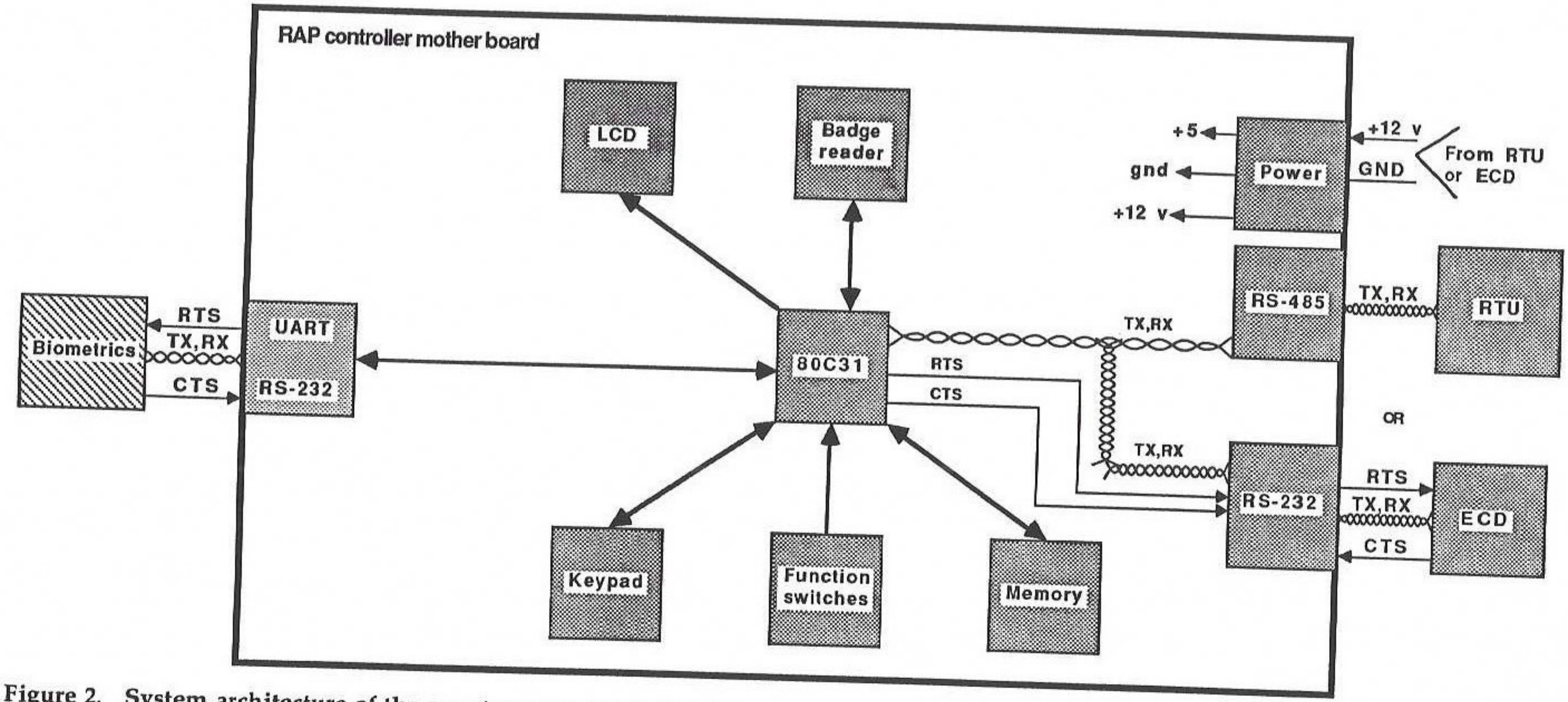


Figure 2. System architecture of the remote-access panel prototype.

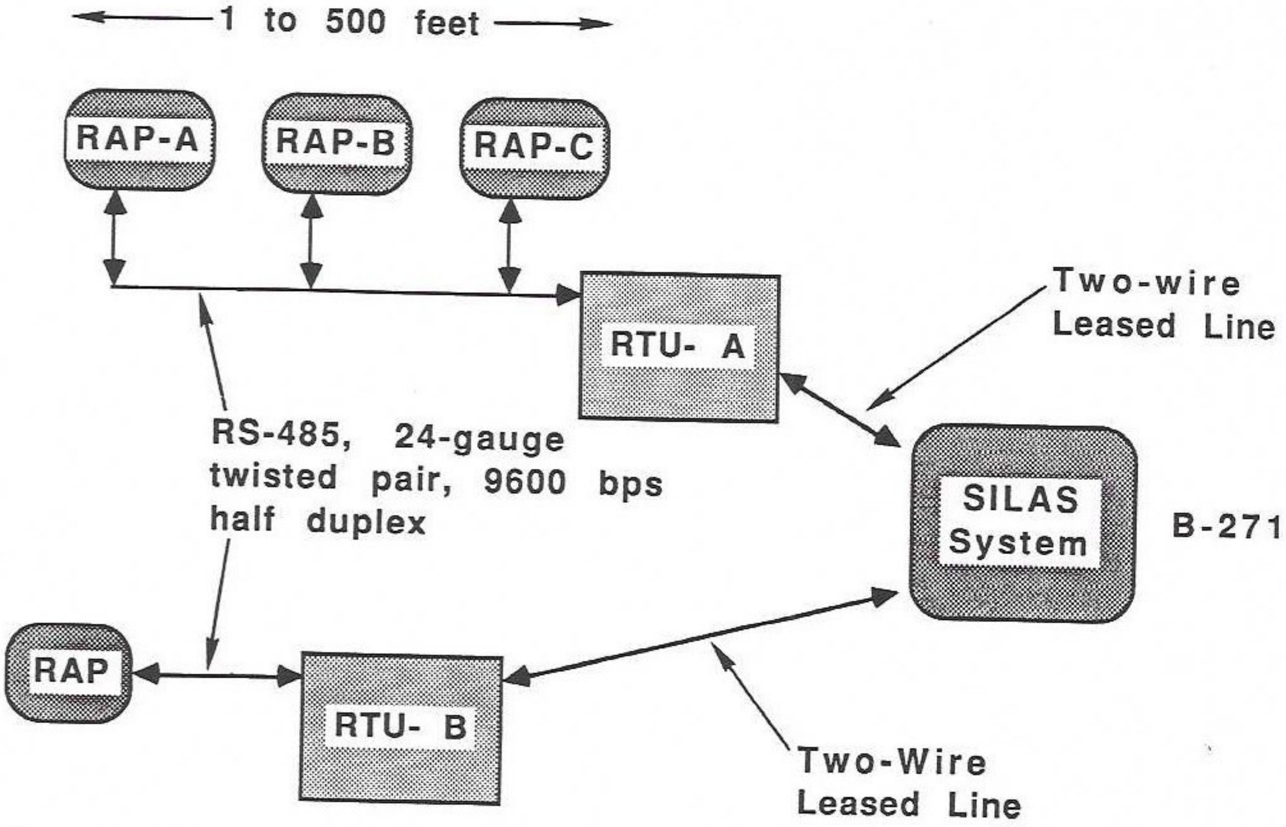


Figure 3. Hypothetical SILAS system configuration.

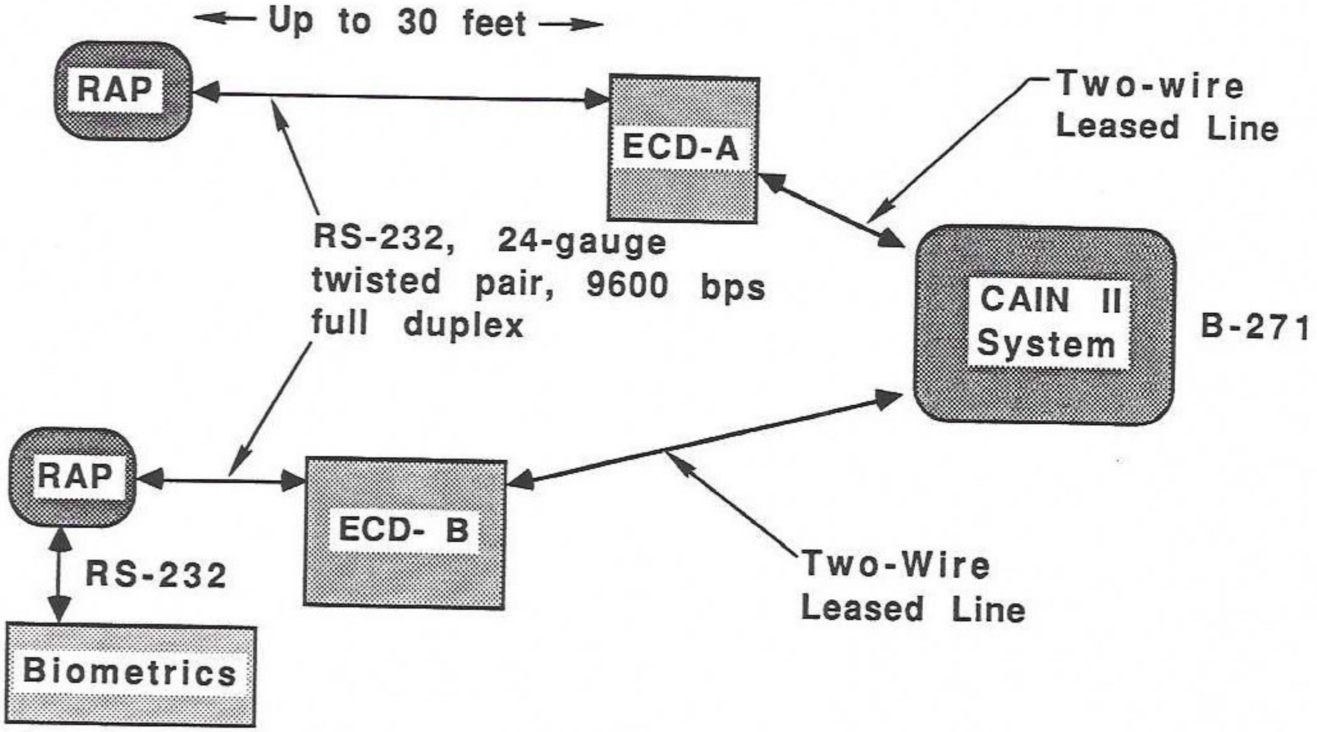


Figure 4. Hypothetical CAIN II system configuration.

finger-print reader or a retinal scanner, used for positive identification of personnel entering highly classified areas.

The SILAS RAP: When the RAP is used in SILAS it could be up to 500 ft away from the RTU and several RAPs may be controlled by one RTU (Fig. 3). We therefore designed the SILAS RAP to connect to the RTU via an RS-485 physical link (rather than RS-232) because of its ability to allow multidropping on a single pair of wires and its greater noise immunity using balanced rather than single-ended transmission. With several RAPs on a line we must be able to address a particular RAP, a need answered by the DIP switch address for SILAS. This line sends and receives information half duplex, at 9600 bps, with the software working on an interrupt basis.

We encrypted the PIN for transfer over the twisted pair to the RTU using the data encryption standard (DES), which the 80C31 has coded in its EPROM. The user's PIN could also be protected by using conduit, but conduit is prohibitively expensive for the distances required in SILAS.

A user of our prototype SILAS RAP can, depending upon his/her privileges, perform the following operations:

- Place a station in access mode.
- Place a station in secure mode.
- Change the station mode to maintenance.
- Display individual sensor status/state.
- Put individual sensors out of service.
- Change the station mode to out-of-service.
- Change the sensor state.
- Change a PIN.
- Enroll a user.
- Disenroll a user.
- Walktest the station.

The CAIN II RAP: The RAP as used in CAIN II (Fig. 4) employs the RS-232 standard physical link, full duplex, at 9600 bps. The CAIN II RAP is closer to the ECD—within 30 ft or so—and there is no need to attach several RAPs to one ECD. Therefore, there was no requirement to encrypt the PIN. A biometric device may be connected to some CAIN II RAPS via an RS-232 serial link and the UART (Fig. 2).

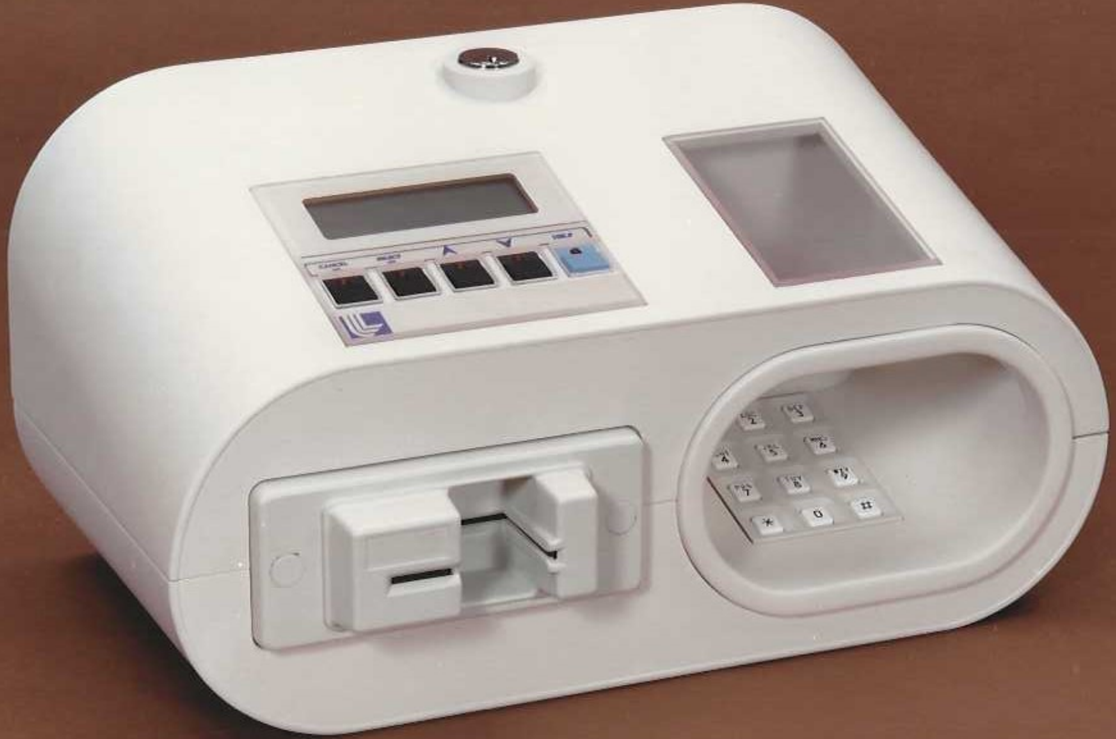
Conclusions and Current Status

This report presents the system design of the RAP prototype from its inception to November 1986. Since that time the SILAS development team has made major changes to both the RAP and SILAS. Some changes to the RAP include:

- Incorporation of a low-power badge reader, eliminating the need to switch power to the reader.
- Modification of some circuitry to improve reliability.
- Modification of user-interaction procedures.
- Complete elimination of the electronic keypad option.

Acknowledgments

We would like to acknowledge the efforts of Woody Souza, Karl Soneson, and Greg Sykora from the SILAS project, Bill MacFarland from the CAIN II project, and Bill Banks and Jim Moore from the Systems Research Group for their very important contributions to the development of the RAP prototype.


CANCEL
SELECT
HELP
2
3
4
5
6
7
8
9
*
0
#