



2355 Mira Mar Avenue  
Long Beach, CA 90815-1755  
562-986-9105  
[www.mercury-security.com](http://www.mercury-security.com)

## Subsystems - Defined

*Understanding the architecture to achieve reliable access control solutions*

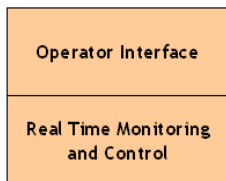
## Access Control Subsystems – Defined

The hardware subsystem is an integral part of any comprehensive access control solution.

Understanding the components of an access control solution– how they function and how they inter-relate to other parts within the system is essential to creating the optimum solution for the end user.

### Anatomy of an access control system

All access control systems share a common structure. On one end are the users – the security guards and administrators who monitor and configure the system. On the other end resides the peripheral hardware – readers, keypads, doors, locks, sensors and numerous other devices where all system users interact. Between each of these ends is the access control system, which enacts and reacts to the demands that are made at either end.



The access control system can be subdivided into two functional layers: the operator interface and the real-time monitoring and control layer. The operator interface is used for configuration, database and general system management, and report generation. This layer is commonly referred to as application software. Since this layer is linked to the users, it can be tailored to meet the requirements for a particular application and client base.



The real-time monitoring and control layer that links the application software to the peripheral devices is commonly referred to as “Access Control Hardware.” In the Mercury model, this layer is a self-contained separate subsystem.

### Access Control System

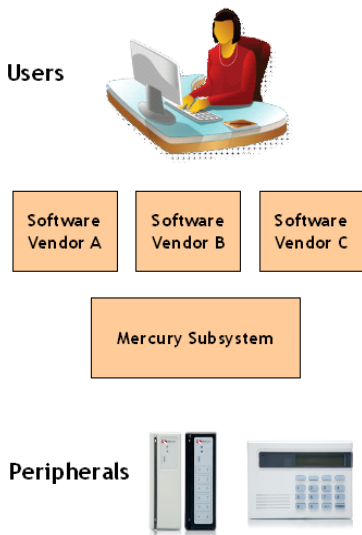
### Advantages of the Subsystem

In traditional Access Control systems, the vendor provides a “complete” package – everything from the application software to the card readers and everything in between.

Historically, the perceived advantage of this single-vendor solution has been one-stop shopping. The disadvantage for customers is that they are locked into a vendor’s system with both hardware and software. The disadvantage for the vendor is that it must devote resources to being both a state of the art software provider

as well as a leading hardware manufacturer, a costly endeavor limiting end user choice to a few large companies financially capable of doing both well.

It was this challenge that changed the face of the computer industry. Historically, mainframe computer vendors provided complete hardware and software solutions to their customers. As the industry evolved, a clear separation between hardware and software vendors emerged. Today software is available from any number of software vendors, and modern hardware vendors supply a full range of products that operate together.



Similarly, it became apparent to the founders of Mercury that the behavior and characteristics of the access control system could be isolated from the application software. By separating the hardware and related “drivers” from the application software, Mercury has defined the subsystem this paper will describe.

By focusing its resources on creating the heart of the access control system – Mercury provides a reliable, flexible and portable subsystem that allows our OEM partners to tailor their solutions to customers’ needs and requirements. Much in the same way that PC hardware and related operating system software are created today.

The architecture of the subsystem allows our partners to develop application software in a stable, well exercised, isolated hardware environment, allowing developers to take advantage of new hardware models with little or no software changes.

### **Access Control Subsystem**

The uniqueness of this architecture lies in the three components or layers of the Mercury subsystem:

- The Application Program Interface (API),
- the Firmware, and
- the Hardware.

### **Application Program Interface**

Mercury’s Application Program Interface (API) bridges the OEM’s access control application software and the subsystem firmware. The API is essentially a software layer that runs on the host computer and is integrated into the application software.

The API has two functions:

- Establish communication with the hardware
- Expose the capabilities of the subsystem's firmware and hardware layers

The language defined by the API provides the stable platform that isolates the access control application from changes in the firmware or hardware. New features in the firmware are added to the API in such a way that the current implementation is not affected. When the software manufacturer is ready to implement those features, the enhanced language of the API is the roadmap for easy inclusion in their systems.

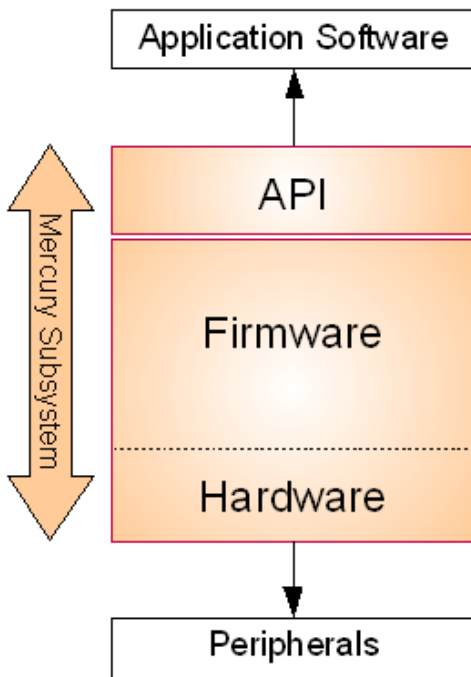
The Mercury API is common for all of our developer partners. As different development projects address different problems in the access industry, our partners are able to create their solution to meet the needs of their customers while giving their product a unique identity. The API ensures that each partner has access to the same feature set of the Mercury platform.

Since the API is strictly a software layer, it is portable to other operating systems and currently runs on the Windows operating system, Linux operating system and MAC OS.

### **Firmware**

Mercury firmware is the intelligence behind the access control subsystem. It receives its configuration and operating rules from the host, and carries them out within the hardware without further intervention. The firmware manages the cardholder database, evaluates access requests against a set of access rules, monitors events and performs additional instructions based on those events, and records a history of all events. That history is processed by the host application and can be used to generate usage reports or signal the operator that something needs attention.

The firmware also isolates specific hardware behaviors from the logic. This isolation makes it possible to add readers and other peripheral hardware without affecting everyday operation. The Mercury subsystem is not tied to a specific type or family of readers.





## Digital Video Recorder with VAP

The manipulation and information management onboard a Mercury controller is known as the Virtual Access Processor or VAP. It is virtual because it can exist anywhere a suitable device can host its potential. The VAP was designed to be portable and independent from the given hardware. Porting the VAP has allowed Mercury to take advantage of new advances in hardware technology, as well as provide unique solutions for installations involving large amounts of legacy hardware.

### Hardware

The hardware layer of the subsystem provides the link to the physical world. Hardware selection is a result of matching the customer's requirements with the physical topology of the installation.

Traditional RS-485 wired devices provide well practiced and highly secure data paths where failures in communication are not well tolerated. IP-enabled devices are popular in installations equipped with highly reliable and secure data networks. These devices can provide installation savings for power and wiring.

The debate over the practicality of IP-enabled devices vs. the security of RS-485 connected devices in ongoing and requires a lot of examination. This debate will have to wait for another time however, as it is not in the scope of this paper.

### Hardware Topologies

Hardware topologies vary based on the characteristics of the physical installation. Mercury created a family of products that allows the security designer to mix and match specific hardware to meet the individual needs of the installation.

### The Mercury Product Family

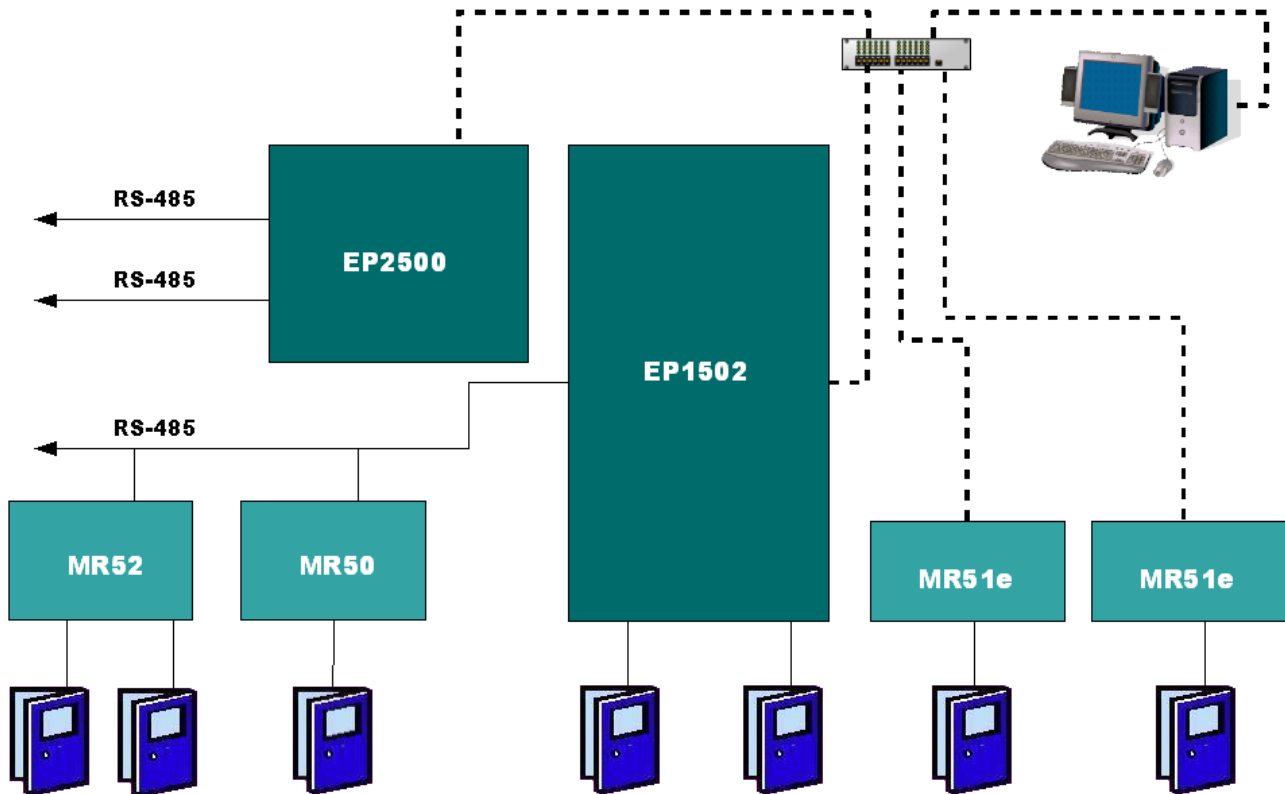
The **EP2500** platform provides an Ethernet ready, fault-tolerant intelligent controller capable of efficiently managing a large network of access panels in any system design.

The **EP1502** is a multi-port controller platform for OEMs, providing a high-performance Ethernet ready, cost-effective intelligent controller and dual card reader panel capable of controlling two doors, with auxiliary point control and monitoring.

The **MR50** is the choice for a low cost, high performance single card reader interface panel.

The **MR52** is a low cost, high-performance device that provides all the I/O needed for controlling two doors with auxiliary point control and monitoring.

The **MR51e** is a single door, network ready interface panel for OEMs. The unit is easy to install and provides the I/O needed for controlling a single door with power over Ethernet for complete door functionality.



**Mercury Product Family Topology**

## Access Requirements

By taking Mercury's subsystem approach to system design, OEMs can readily provide customers with access control systems that achieve essential characteristics:

- Reliability
- Availability
- Interoperability
- Interdependency

**Reliability** means that the system has undergone rigorous testing and has proven performance. Reliability can be measured in percentage up-time or mean time between failures. With more than one million installed panels, Mercury sets the standard for reliability.

**Availability** means reliable operation in a timely manner. Mercury products are designed to provide fast response even under the most severe load conditions.

**Interoperability** is the ability to connect to different technologies, such as display devices, keypads, biometric readers, wireless devices and smart cards. Mercury supports a variety of reader protocols and display devices—clock/data, Wiegand, and RS-485.

**Interdependency** addresses the range of equipment whose operation must be coordinated. For example, anti-passback rules may require tracking a user's movements between doors. The decision to grant or deny access may depend on events that happened at different doors. Using if/then logic, the Mercury subsystem provides this interdependency, triggering on events that happen at one door to affect other doors.

The higher levels of performance and integration obtained in the Mercury subsystem provide a cost-effective platform on which our partners can base their business. Together our partners and the end users reap the benefits of a large installed hardware base, meet the demands of today's market, and enjoy an economy of scale that could not be achieved individually.

