Introduction

The Institute of Electrical and Electronics Engineers defines a system as “a collection of components organised to accomplish a specific function or set of functions” [IEEE STD 610.12]. With this in mind, a system plan at a port must outline and define the function (or set of functions) and goal(s) of the system. Two of the largest and sometimes most important systems at a port could arguably be the terminal operating system (TOS) and the gate or port access control system (PACS).

A common misconception is that an optical character recognition (OCR) system is the PACS. Nothing could be further from the truth. An OCR system is an optional subsystem of the modern PACS, it is not the core of the PACS. The core of the PACS is the database solution, for example access control software built on a commercial database platform. Whether or not OCR is used and how it is used depends completely on the business process of the facility. Access control systems depend on a set of parameters and data collection systems such as RFID, OCR or biometrics. Given that the PACS is the system at the center gate operations, we must define the system functions as described by the IEEE and ask the question, “Is OCR the right technology to achieve the function(s) of the system?”

Traditionally in many operations the PACS served as a subsystem designed primarily to supply information to the TOS. Simply supplying information was adequate because of the business process of the facility. This type of PACS might have included OCR for container and license plate recognition (LPR), RFID, and a perhaps a manual process. Access permission to the port was based on LPR reads, RFID numbers, or another standard means. Information was sent directly to the TOS with one interface for each technology. Today, such a traditional approach to a PACS would be costly, inefficient, and probably ineffective for a port to serve their customers and stay ahead of competitors in the market.

Design and technology

The system design of a modern PACS is different from a traditional access control system in many ways. An international port has much different access control requirements than a bank or even a government building. A true PACS must be able to manage access and area control, parking permits and ID cards, employees of the port, terminals and restaurant staff, access to the customs area and the terminals, commercial traffic, public traffic, red carpet customers, trailers, trains, cars, bicycles, pedestrians, ship crews, maintenance crews, taxis, and emergency vehicles and personnel (just to name a few). Furthermore, at any given moment during the day or night, there are tens-of-millions of EUR’s of cargo and equipment on the premises and there can be...
competing terminals with highly sensitive business information located next to each other. Each port also has a variety of specific needs depending on ISPS code requirements and other local factors. Overall this makes the PACS one of the most complicated access control systems in the world.

Due to the significant growth seen in the industry over the last few years, rising concerns over security, and other business issues, a separate database for the PACS makes a lot of sense. The database platform must be reliable, flexible, and scaleable. Given such requirements, a well-known, commercial database is a good choice. The network must also be able to handle demanding requirements. TCP/IP is an appropriate selection. The end-user benefit of a commercial database PACS communicating over TCP/IP is very clear: It is virtually impossible for even the world’s busiest ports to overload the system with traffic events and online users. That is, literally 1,000’s of traffic and access control events can be happening at the same time with a virtually unlimited number of users in the system without queuing data streams adversely affecting port performance.

The PACS can communicate directly with a TOS (or multiple TOS’s), customs agency system, external databases, or any other system with a direct interface. The reduction of interfaces leads to a massive increase in efficiency of port operations via a simplified system. The overall system architecture can be designed so that multiple TOS’s (even for competing terminals) interface with a single PACS. The single PACS can interface directly with the customs system making the PACS the center of port operations. With the help of traffic guidance as part of the PACS, truckers can make multi-terminal visits and clear customs authorities in a single trip before exiting the port.

Additional technologies can be added to the PACS as access control devices (i.e. Mifare cards, PIN code readers, or biometric devices) or as another means to support the business process at the gate (i.e. scales, high-resolution damage inspection portals, or overview pictures of the event). By integrating these technologies at the PACS level, no additional work is required by the TOS for the interface. Furthermore, all event information is stored together and can be viewed on one user interface.

Conclusion

There are many technologies that go into a PACS. For maximum efficiency of gate operating procedures, theses technologies should be built on a reliable database platform that has only one interface to each external system such as the TOS or the customs system. Before selecting technologies for the PACS, it is good business practice to first define the system function and outline the goals of the system with respect to the business process. Once there is a clear definition of the functions, selecting the technologies is relatively simple and because the PACS is built on a reliable database platform it will be completely scalable in design and able to grow with the demands of the industry. New technologies can be added or old technologies can be removed without additional work from the TOS supplier. In practice this means that a two traffic-lane system can be scaled-up to include 100’s of lanes and checkpoints on a single network without having to replace the PACS. This long term vision in PACS design will benefit ports for many years to come.

ABOUT THE AUTHOR

John Lund is the International Sales Manager for Visy Oy in Finland. He is a graduate of Northeastern University, Boston USA, Rochester Institute of Technology, Rochester, NY, USA, and the Defense Language Institute, Monterey, CA, USA. His background includes consulting projects for ports and logistics centers, and the application of western economics to businesses in transition economies.

ABOUT THE COMPANY

Visy is a high performance software company specializing in access and area control solutions for port authorities, public and private logistics terminals, customs agencies, and government organizations. Visy has designed and implemented the largest customs agency OCR system with an alarm database solution between the EU and the east (Finnish Customs Agency), the largest port authority access control system in northern Europe (Port of Kotka, Finland), and Visy provides access control and OCR systems to Fortune Global 500 companies such as StoraEnso.

ENQUIRIES

Visy Oy
Pyynikintie 25
Tampere FI-33230
Finland
Tel: +358 (0)3 211 0403
Fax: +358 (0)3 211 0402
Email: sales@visy.fi
Website: www.visy.fi