PCS*express* makes development, accreditation, deployment, operation and maintenance of high-assurance distributed systems affordable. The MILS architecture significantly increases the protection, reduces time to develop, and reduces schedule risk of deploying technology to provide high assurance systems that are both safe and secure.

PCS*express*™

Objective Interface Systems, Inc.

Objective Interface is leading the MILS middleware development process in collaboration with its partners, including the National Security Agency, U.S. Air Force Research Laboratory, the University of Idaho, Lockheed Martin, Boeing, Raytheon and Rockwell Collins.

Objective Interface is the worldwide leader of real-time, embedded and high-performance communications middleware. The company's products include ORB*express*®, based on the Common Object Request Broker Architecture (CORBA), DDS*express*™ a publish-subscribe technology based on the Data Distribution Service standard (DDS), and PCS*express*™, secure communications middleware for MILS architectures, to meet the high-performance requirements of military and aerospace, transportation, telecommunications, data communications, robotics, consumer electronics and industrial automation and process control.

Objective Interface products, sold worldwide, are used in a variety of real-time, high-performance and embedded applications, including communication systems, mission-critical avionics systems, network management, vehicle control and management systems, software defined radio, telecommunication systems, process control systems and nuclear fusion ignition facilities.

Contact Info

Corporate Headquarters:
Objective Interface Systems, Inc.
13873 Park Center Road, Suite 360
Herndon, VA 20171-3247
U.S.A.

www.ois.com

OBJECTIVE INTERFACE™

For more information,

visit: mils.ois.com,

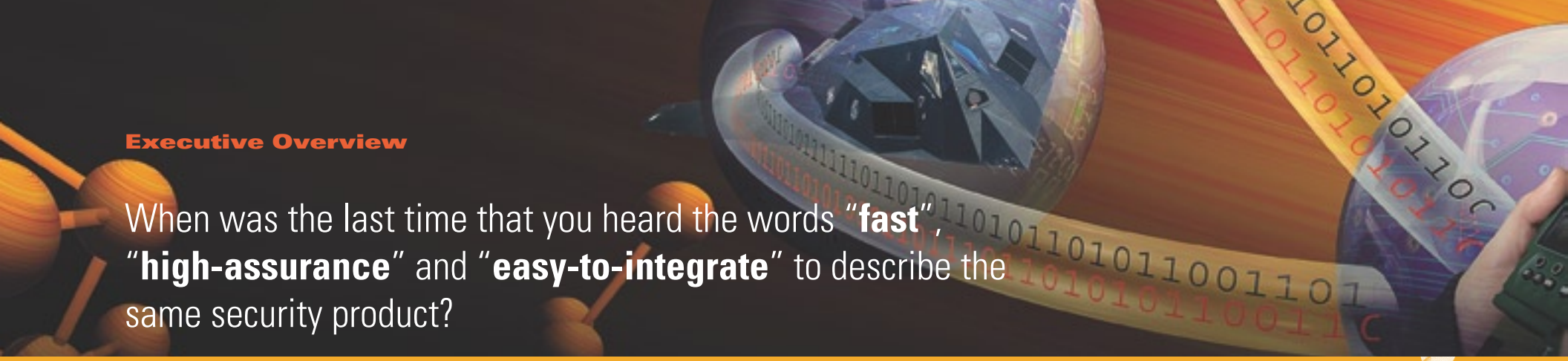
call 1-800-800-OIS7 or +1 703-295-6500,

or e-mail inquiries to: info@ois.com.

OBJECTIVE INTERFACE™

PCS*express*™

for Military and Aerospace



Executive Overview

When was the last time that you heard the words "**fast**", "**high-assurance**" and "**easy-to-integrate**" to describe the same security product?

System integrators are under increasing pressure to provide strong security for their systems, while providing greater functionality and flexibility to the Warfighter. At the same time budget pressures dictate that programs have fewer dollars to spend.

PCS*express*™ is the definitive implementation of the MILS Partitioning Communication System architecture. PCS*express* saves size, weight, and power while reducing certification and accreditation costs.

PCS*express* provides complete control of each information flow between applications in a distributed system. PCS*express* provides high robustness separation of data throughout network communications.

PCS*express* is high-assurance COTS security software to build high-performance, GIG-connected Cross-Domain Solutions. Objective Interface developed PCS*express* specifically for high assurance certification, including:

- Common Criteria EAL 6+
- DCID 6/3 PL 5
- DO-178B Level A

OBJECTIVE INTERFACE™

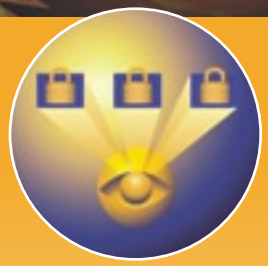
Why PCS*express*▸ ?

▶ PCS*express* Protects Investment in Legacy Applications

PCS*express* allows legacy network applications to run without change. PCS*express* makes communication security transparent to the application, middleware, and network protocols. PCS*express* operates independently of traditional middleware such as CORBA, DDS, SQL, Web Services, .NET and others. PCS*express* allows for the continued use of existing middleware solutions to develop and deploy applications. Existing code bases and libraries can remain essentially unmodified even though security requirements have changed or increased.

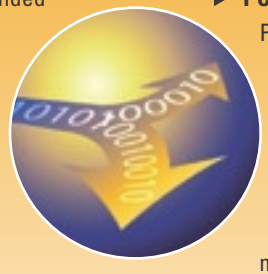
▶ PCS*express* Simplifies Secure Application Deployment

PCS*express* lets each developer concentrate on his application without worrying about securing how that application communicates. Architects draw systems as functional boxes connected by data flow arrows. PCS*express* guarantees data can only flow along those arrows, and that there are no unintended arrows. Information flow between functional boxes can be trusted. The communication system cannot introduce unwanted side effects. The PCS*express* damage limitation capability isolates obscure application bugs such as accidental bandwidth overrun. This modularization of concerns lets each developer concentrate on the behavior to be implemented, reducing schedule uncertainty and risk.



▶ PCS*express* is Easy to Administer

Each user community can independently control system authorization and manage its own security. Security enforcement is automatically coordinated.



▶ PCS*express* Enables Coalition Force Operations

PCS*express* makes it easy to create and connect a wide variety of communities of interest on a secure basis. This means that for the first time, coalition force network operations can easily separate the communication between coalition partners so that each partner can quickly access authorized information without manual intervention.

▶ PCS*express* Reduces Certification and Accreditation Risk

PCS*express* was designed and implemented following NSA guidelines for High Robustness certification. PCS*express* reduces schedule and cost risk for certification and accreditation.

▶ PCS*express* Allows Quick Reaction to Changing Requirements

Changes in infrastructure and communications security requirements are accommodated without changes to the application because communication channel security is independently administered.

▶ PCS*express* Allows Agile Networking

PCS*express*' ability to bridge between networks and across domains provides the capability that Network Centric Operations (NCO) demands. This capability allows the Warfighter to leverage information supremacy.

What Is MILS?

MILS, *Multiple Independent Levels of Security*, enables affordable, high-assurance application-level security. The MILS architecture creates a high assurance foundation by combining small, mathematically verified software components.

The MILS architecture was developed to resolve the difficulty of certification of high assurance systems, by separating out the security mechanisms and concerns into manageable components. MILS applications are empowered to enforce domain-specific security policies instead of relying on overly generalized security kernel services.

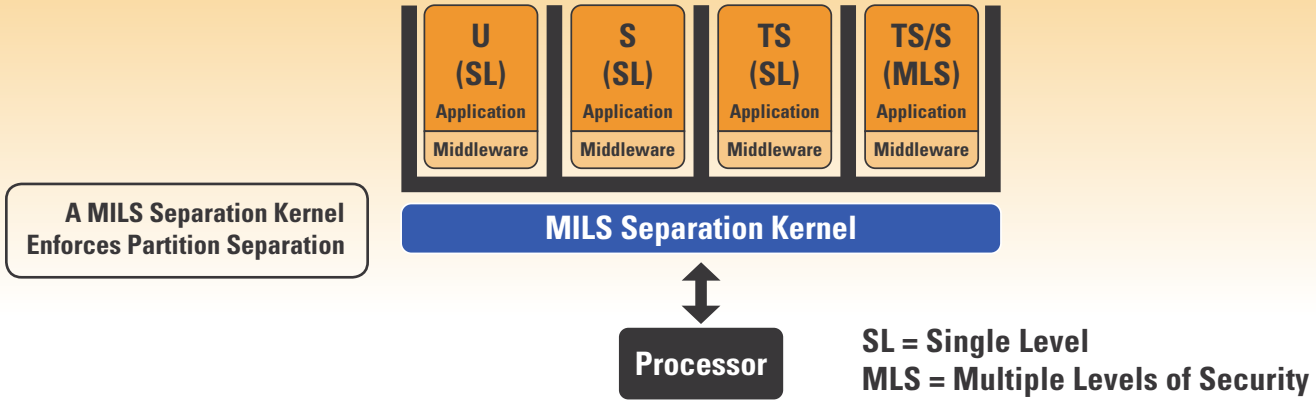
A small Separation Kernel, the core of MILS, provides trustworthy security boundaries while simultaneously controlling the flow of information across those boundaries *on a single computer*. A Partitioning Communication System, a crucial part of the MILS Middleware, controls the flow of information *among multiple computers*.

The MILS Separation Kernel and Partitioning Communications System make *mathematical verification* possible for the core systems software by reducing the system security functionality to four key security policies:

- **Information Flow** — Information originates only from authorized sources, is delivered only to intended recipients, and the source of information is authenticated to the recipient. Flow is controlled within a single processor and end-to-end in distributed systems.
- **Data Isolation** — Information can only be accessed by authorized subjects. Private data remains private.
- **Periods Processing** — The microprocessor itself is not a covert channel, leaking information as it switches from partition to partition. The distributed system will not leak information as a side effect of authorized usage.
- **Damage Limitation** — A failure in one partition does not cascade to another partition. Failures are detected, contained, and recovered from locally.

Because of the controlled information flow, applications can enforce their own security policies with a guarantee that they are non-bypassable. Distributed components can only interact in proscribed ways, eliminating unanticipated side effects.

The MILS architecture frees most application code from the requirement for rigorous security analysis. MILS application code cannot attack or be attacked by unrelated applications.



A MILS Separation Kernel Enforces Partition Separation

SL = Single Level
MLS = Multiple Levels of Security

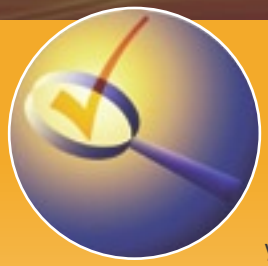
What is PCS*express*?

PCS*express* is Secure Communications Infrastructure

PCS*express* is high-performance, real-time communications software that provides securely separated communications channels between systems.

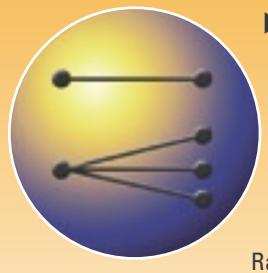
PCS*express* is Key to Multiple Independent Levels of Security (MILS)

PCS*express* is a critical component of MILS that extends the Separation Kernel's policy enforcement to distributed systems.



PCS*express* is High Assurance

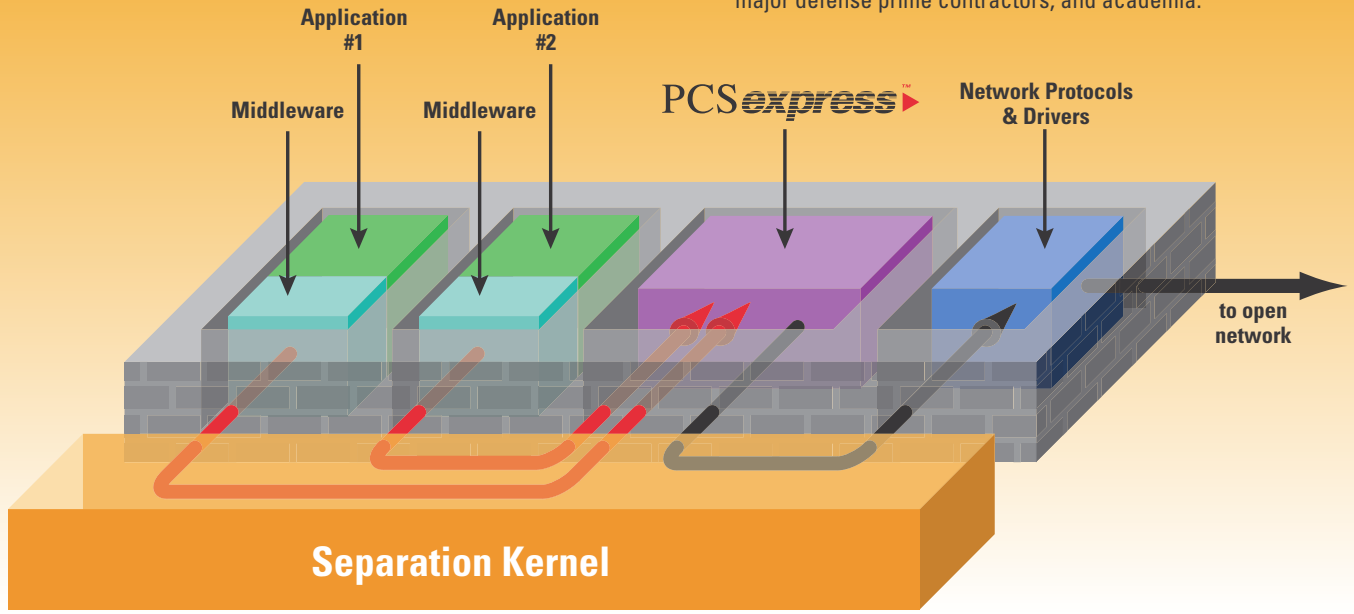
PCS*express* is high assurance COTS middleware, the highest levels of the Common Criteria. With PCS*express*, the communications security policy is enforced by a component that is based upon years of research by Objective Interface in cooperation with the Department of Defense, major defense prime contractors, and academia.



PCS*express* is Independent of Communications Protocols

PCS*express* enables secure inter-system communications and strong node/application authentication over a wide variety of communication protocols including:

- point-to-point (*e.g.*, TCP, UDP, SCTP, RapidIO, Infiniband, VME, PCI, et al) and
- point-to-multipoint (*e.g.*, IP Multicast, FireWire, USB, Link16, et al).



PCS*express* protects applications from the network and the network from applications

Functional Properties of PCS*express*

PCS*express* Enables High-Performance Communications

The total zero-copy architecture optimizes the performance of network communications and minimizes security overhead. Latency (delay for delivering the first byte) and bandwidth reduction (delay added to each additional byte) are optimized specifically for each Separation Kernel platform. Exhaustive benchmarking has shown that bandwidth is most severely constrained by the number of times that data buffers are copied by applications, stacks, and middleware. Objective Interface has worked directly with each Separation Kernel vendor to implement secure data transfer between partitions without copying.

PCS*express* Enables Fault Tolerant Systems

The PCS*express* design precludes a single point of failure. This means:

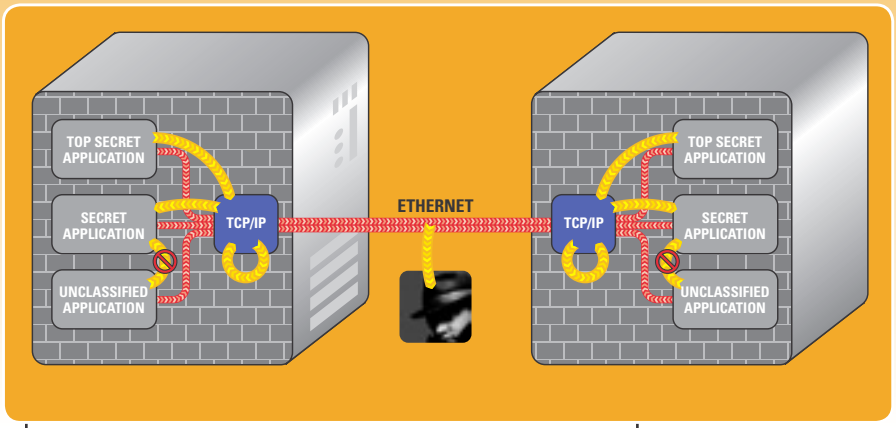
1. the PCS*express* security infrastructure safely survives node and communication link failures *and*
2. system architects can configure applications that survive node and communication link failures.

PCS*express* Enables Agile (and Secure) Network Configuration

PCS*express* provides safe and secure dynamic addition and reconfiguration of deployed, active channels. This enables systems to react quickly to changing requirements and facilitates Network Centric Operations.

PCS*express* is Application Transparent

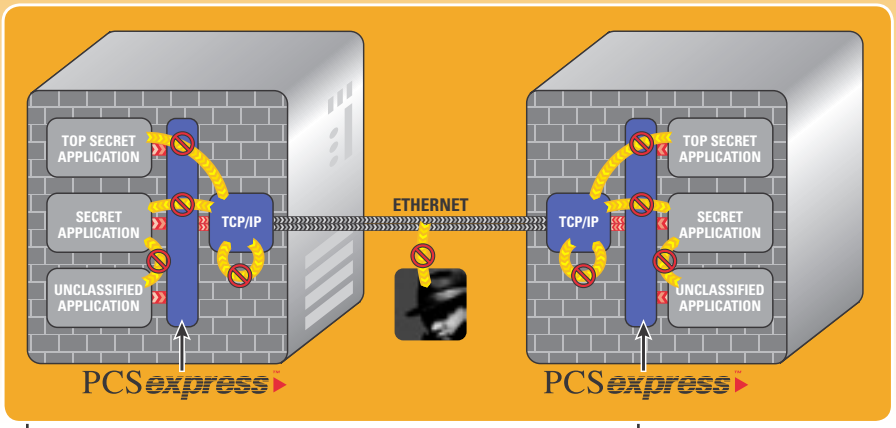
The strong security capabilities of PCS*express* are provided in a form that isolates application code from the complexity of the security functions (identification, authentication, authorization, policy administration, etc.). Thus, applications can evolve independent of the security function. The administration of the security function is independent of the applications.



Without PCS*express* MLS Communication Between Separation Kernels is Subject to Many Threats

MILS Separation Kernel

Threats



PCS*express* Counters These Threats by Securely Separating Information Channels

MILS Separation Kernel

Threats

Security Properties of PCS*express*

PCS*express* Enforces Information Flow

PCS*express* allows security administrators to set security policies as explicit information flows between robustly separated subjects. Information flow-based policy administration is simpler and more adaptable to changes in requirements.

PCS*express* Safeguards Information Flow

PCSexpress communication channels are protected with high assurance.

- PCSexpress performs strong node and application authentication before data is allowed to flow.
- Bandwidth allocations are enforced guaranteeing quality of service. Covert timing and storage channels are suppressed.
- Distributed key supercession and promotion of key generations to deployed systems ensure confidentiality and integrity of data.
- Forward secrecy for group and point-to-point communication is maintained.

The bottom line is that applications can communicate more securely without implementing additional security functions.

PCS*express* Provides Trustworthy Separation

With PCS*express*, multiple physical networks are no longer required to guarantee that data with different security levels (TOP SECRET vs. SECRET) or belonging to different Communities of Interest (SECRET NOFORN vs. SECRET NATO) will remain separate. PCS*express* cryptographically separates multiple data flows. Duplicate "air gap" communication links used to ensure separation can now be collapsed down to a single physical channel based on COTS networking equipment. Traffic on one logical flow cannot affect, or even be detected by, the parties exchanging data on any other logical flow. Projects realize significant savings in size, weight and power as well as cost.

PCS*express* is NEAT!

The Separation Kernel foundation plus the high-assurance engineering process that produced the PCS*express* software means that PCS*express* is:

- **N**on-bypassable—the security functions cannot be circumvented
- **E**valuatable—the security functions are small enough and simple enough to be mathematically verified and evaluated
- **A**lways invoked—the security policy is enforced each and every time
- **T**amperproof—subversive code cannot alter the operation of the security functions by exhausting resources, overrunning buffers, or other forms of making the security software fail

PCS*express* Enables Layered Assurance

PCS*express* provides a robust communications foundation guaranteeing that distributed downgraders, guards, and firewalls cannot be bypassed. Complex systems can then be decomposed into functional modules that can interact only in predictable ways. Because of this certainty, each module can be individually evaluated and certified, simplifying system accreditation and maintenance.

PCS*express* Enables Distributed Management of Security Policies

PCS*express* robustly supports independent management of distributed authorizations. Centralized policy management is not required. Each user community can independently specify and manage their own security policies including constraints on policy interaction. Policies are automatically combined to control authorization.

PCS*express* Enables Secure Communications Over Untrusted Networks

PCS*express* assumes that the network is not trustworthy. Data is safeguarded before it is placed in the custody of the communications infrastructure. Not relying upon the network to have any security properties enables the system designer to utilize COTS protocol stacks, network interfaces, transmission media, hubs, switches, and routers without exposing distributed data to additional threats.