



STOP™ Version 7

Platform for Secure Cross-Domain Application Development

Working to become a dependable partner of choice

BAE Systems Insyte's information security products enable classified information sharing, while enforcing network segregation. Highly evaluated, these products provide unrivalled data security and are available off-the-shelf or as part of a total system solution.

The Secure Trusted Operating Program Version 7 (STOP 7) is the next generation operating system (OS) and provides the ideal platform for developing and deploying high assurance, multilevel secure applications. STOP is the OS for BAE Systems' XTS line of products.

STOP 7 is an upgrade to its predecessor, STOP 6, providing robust security and access control, enhanced processing speed and network performance, and the portability to be deployed in any environment, from the server room to the tactical edge.

STOP 7 is designed and developed by the same team of security engineers who produced STOP 5 and STOP 6 on the XTS-300/XTS-400 hardware platforms. STOP 6 is the highest evaluated general purpose OS in the world, achieving the Common Criteria Evaluation Assurance Level 5 Augmented (EAL 5+).

STOP and the XTS line are the underlying OS and platform for over 700 cross-domain deployments worldwide.

Secure Operating System

STOP 7 is designed and built from the ground up with security as its primary feature. This allows for complete and consistent control over security features and functions, providing a level of assurance above and beyond those offered by "hardened" operating systems. Designed and developed to achieve EAL 5+, customers can be confident that data may pass from one security domain to another in absolute compliance with the specified security policy.

STOP 7 is engineered to meet the evolving needs of the cross-domain industry, incorporating top-notch performance, hardware and platform flexibility, and enterprise-class security features. The networking, processing, and file access speeds of STOP 7 rival or exceed those of commercial off-the-shelf operating systems, resulting in the ideal platform to host real-time, high-performance and heavy-load solutions vital to military, coalition, and interagency data sharing.

Security Controls and Features

STOP 7 incorporates a 2-ring architecture to protect data and functionality. The kernel ensures that information, processes, and devices stored and running on the system cannot intermingle in violation of the system's mandatory security policy.

Access control mechanisms available to the secure solutions engineer include two types of Mandatory Access Control (MAC):

- **Multi-Level Security (MIS):**
Incorporating the Bell-LaPadula security and Biba integrity models (BL/B), STOP 7 labels all objects on the system with sensitivity and integrity levels and optionally, sensitivity compartments. This mandatory, hierarchal security policy utilizes sensitivity levels to protect data from unauthorized (lesser cleared) access, while protecting processes, configuration data, and logs from attacks on the system's integrity.
- **Role-Based Access Control (RBAC):**
New to STOP 7, RBAC provides a powerful, flexible access control mechanism allowing unprecedented granularity in architecting security policy for enforcement on both data and users. RBAC allows the security architect to tie specific actions to specific object and subject combinations, providing absolute isolation of subsystems or groups of objects from other parts of the system.

In addition, Discretionary Access Control (DAC) allows for simple configuration of read, write, and execute of objects to users and groups.

Multi-Level Secure Solutions

The STOP 7's Linux® -like programmatic interfaces enable developers to port or develop applications easily on the system. These applications primarily reside outside the system's Target of Evaluation (TOE), making them easier to certify and accredit while deriving a high degree of security and integrity from the underlying mandatory protection mechanisms in the TOE.

As applications on the XTS have been repeatedly certified, accredited, and deployed in highly sensitive cross-domain environments, STOP has a proven track record of providing the necessary security framework and has the pedigree critical to achieving future Approvals to Operate (ATO).

STOP 7 is designed for federal government use, specifically to host multi-level and/or cross-domain applications. As such, certification and approval features are inherent in its functionality, including MAC, authentication, principle of least privilege, separation of roles, auditing, and others.

Flexible Deployment Options

STOP 7 is designed to be portable, flexible, and mobile in its deployment options. The OS can be deployed on a wide variety of platforms, beyond traditional server environments, including:

- Single-board Computers (SBCs)
- Virtual Appliances
- Embedded Devices.

This hardware flexibility opens the door to tactical deployments such as on board aircraft, in command vehicles, in backpacks, and other areas. These options are critical to current and future tactical information sharing programs, particularly those with real-time, cross-domain requirements. In addition, STOP 7's combination of features and performance allow for a wide range of application possibilities, from traditional guards to file servers to network routing.

Life-Cycle Engineering Expertise

BAE Systems has a Cross-Domain Engineering (CDE) group that specializes in the development of data guards and other security applications that run on STOP and the XTS platform. The CDE team is experienced in the entire life cycle of development, including requirements analysis, development, documentation, certification, deployment, and support. They can help field the systems by providing installation, configuration, accreditation support, training, and help desk support to enable the customer's XTS system to meet their mission requirements.

STOP 7 Key Features

Security

Targeted to industry's needs — military, government, coalition

Performance

Supporting today's real-time, high-performance requirements

Hardware Flexibility

Broader deployment options, cutting edge platforms

Simplicity

Simplified kernel architecture

FOR MORE INFORMATION CONTACT:

BAE Systems Integrated System Technologies Limited
Victory Point
Lyon Way, Frimley, Camberley
Surrey, GU16 7EX, United Kingdom
Telephone +44 (0) 1276 603000
Fax +44 (0) 1276 603001
email insyte@baesystems.com
www.baesystems.com/insyte

Copyright © BAE Systems 2010. All rights reserved.

This publication is issued to provide outline information only which (unless agreed by BAE Systems in writing) may not be used, applied or reproduced for any purpose, or form part of any order or contract or be regarded as a representation relating to the products or services concerned. BAE Systems reserves the right to alter without notice the specification, design, price or conditions of supply of any product or service.

Approved for Public Release by BAE Systems 12/2007

08.10.Insyte.BC433510.01.d01