# System Level Red/Black Separation-A System Level Approach

By Chris Douglass, Project Manager at Orion Technologies

With the increase of data security threats, many new government programs and agencies are calling for more robust methods of mitigating data breaches. Many specifications for embedded computing, including the NSA/NATO TEMPEST certification, require a design architecture that allows sensitive information to be compartmentalized. This is often called "red/black separation". Red/black separation is generally implemented with a thorough segregation between circuits and equipment used to carry plaintext classified or sensitive information that isn't encrypted (RED) with secured circuits and equipment that carry encrypted information (BLACK). Manufactures of TEMPEST-approved equipment must be built under strict standards to ensure that each unit is identical to the unit tested. Even the smallest change or inconsistency can invalidate tests. There is a spectrum of approaches available to address red/black separation.

For cost-sensitive applications that are least demanding in terms of security and performance, a pure-software approach may suffice. Some Operating Systems (OS) support Multi-Level Security, whereby the OS is responsible for enforcing restrictions on access to information by its users and services. This software virtualization scheme may be employed by using a Hypervisor to provide partitions between several OSes running on the same system, but a potential compromise of cryptographic keys has been demonstrated by hostile code running on a Virtual Machine sharing a processor with the security-sensitive process. Some multi-core processors can provide a measure of segregation between cores, but this approach is typically vulnerable to the same attacks on shared resources as Virtual Machines. All of these software-based approaches impose complexity in software and configuration that may have significant impacts on performance and may impose an administration burden to maintain and update in the field.

A higher degree of separation may be achieved with a dual-processor Single-Board Computer (SBC), which essentially packages two individual computing systems on one board. In general, these must be 6U boards to afford the necessary area for two separate processor subsystems, and are not appropriate for systems with smaller envelope requirements. Additionally, the backplane connection often provides relatively limited I/O for each processor.

The most effective way to assure red/black separation is to design a partitioned system on the most fundamental level. While providing a much higher level of information safety than pure-software approaches, a physical partition affords the flexibility of defining the form factor and size of the system based on smaller, common form factor SBCs. Using separate, but smaller

compute modules can often leverage existing COTS modules, and provide an easy upgrade path for a system throughout the life-cycle of a program while not limiting a user to a specific SBC. As new revisions of boards or the next generation of processors are available for an SBC, this system level approach allows the flexibility for an easy and efficient upgrade.

Systems like those designed by Orion Technologies provide advanced backplane designs with red/black separation along with a physical barrier with EMI gasketing along all walls of the system providing further EMI partitioning (see Figure 1 below). These systems are available in ¼, ½, ¾ or full ATR chassis sizes or can be customized to meet specific envelope and environmental requirements and can house either 3U or 6U cards. Orion also can provide a customized front panel to meet specific I/O requirements and offers advanced thermal analysis and testing services.

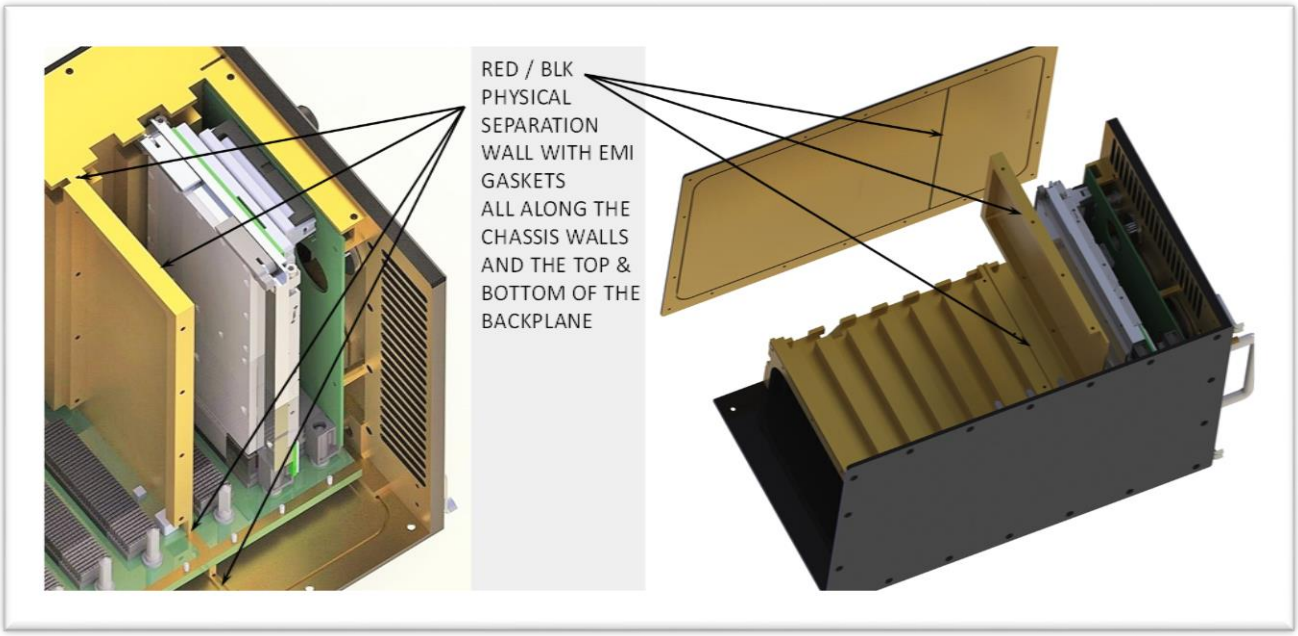


***Figure 1***

## About Orion Technologies:

Orion Technologies, LLC has specialized in the design of embedded electronics for over 20 years. Product offerings include both commercial off the shelf (COTS) and custom solutions to satisfy military, industrial, and commercial requirements. Orion provides customized single board computers, backplanes, power supplies, test equipment and rugged deployment chassis as well as full integration services. Orion places the customer at the center of the business, allowing them to design the most appropriate, affordable solution for each unique application. Orion maintains a dedicated workforce allowing for superior control of the total business process from the initial customer inquiry, through design & integration, to shipment of the final product. Orion strives to not be a supplier but a partner, forming relationships that allow them to better serve their partners. Orion can support singular low quantity projects or high volume, long-term programs. Website: www.oriontechnologies.com