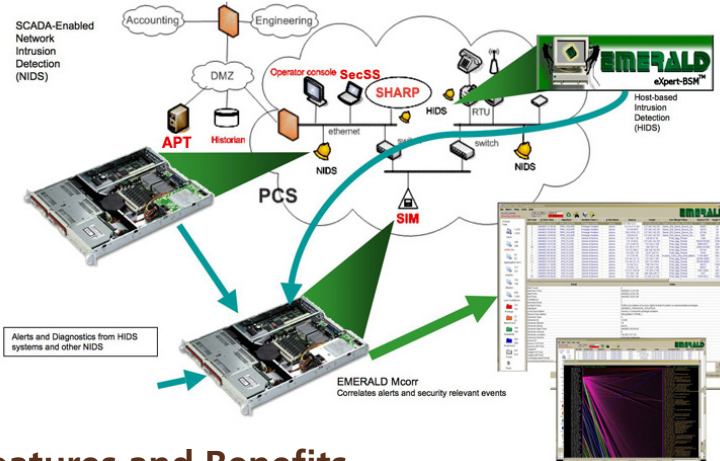




# EMERALD

## Overview

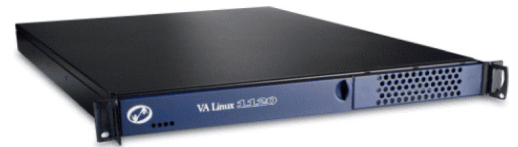
EMERALD is a system for intrusion detection and alert correlation that has been adapted from enterprise networks for use in control systems. It observes traffic at appropriate points in the control network, and analyzes the traffic via a diverse suite of detection algorithms. The detection algorithms are presently aware of Modbus, and permit the user to specify allowed communication patterns. The EMERALD appliance is a network intrusion detection system (NIDS) that uses these algorithms to adaptively determine the PCS's system behavior and detect and report significant deviations. The appliance also accepts and correlates alerts from other sensors in the PCS network (including itself), which can then be viewed via an Alert Management Interface (AMI).



### What is an Intrusion Detection System?

Intrusion detection is the process of detecting attempts to gain unauthorized access to a network or to create network degradation. This unauthorized access is dealt with either automatically or through manual intervention based on a set of rules. IDSs are typically either host based or network based.

Host-based IDSs (HIDS) are software agents used to secure critical network servers and desktops that contain sensitive or critical information. Network-based IDSs (NIDS) monitor activity on a specific network segment. Unlike host-based agents, network-based systems are usually dedicated platforms with two components: a sensor that passively analyzes network traffic and a management system that displays alert information from the sensor and allows security personnel to configure the sensors.



## Key Features and Benefits

EMERALD NetIDS Appliance is the network security administrator's most powerful tool to detect malicious or suspicious activity entering or exiting their networks. It incorporates the following features:

- **Unparalleled breadth of coverage** – No single IDS sensor can out-detect a multi-algorithm IDS. EMERALD NetIDS Appliance's three complementary sensor engines cover the equivalent of approximately 1,000 rules and 20 protocols:
  - Stateful protocol analysis sensor using SRI's forward-chaining inference engine to reconstruct sessions and transactions for HTTP, SMTP, FTP and other application-layer traffic.
  - Anomaly detection sensor using SRI's Bayes Network reasoning engine on TCP sessions to detect probes, scans, floods, denial of service, unusual new services, and unusual inbound or outbound traffic.
  - Stateless packet matching sensor using an SRI-hardened version of the open source SNORT filter engine to analyze TCP/IP information.
- **Dynamic sensor learning** – continuously self-adapts to user's site traffic to detect anomalous patterns and malicious behavior for which specific rules may not exist.
- **Alert correlation** – condenses alert information by a factor of 3 to 10<sup>4</sup> relative to standard IDS sensors.
- **Unauthorized protocol detection and exfiltration** – detects new services tunneling in or out through port 80.
- **Advanced visualization** – EMERALD's Alert Management Interface categorizes incidents by incident class. SRI's unique "discern intent" maps identify hotspot targets and sources that visually identify highest threat alerts.

	SNORT	Commercial	EMERALD Perimeter Defense
Ease of Setup and use	Med	No	Yes
Up to 10 <sup>4</sup> Alert Volume Reduction	No	Some	Yes
Packet Analysis	Yes	Yes	Yes
Stateful Protocol Analysis	No	Some	Yes
Anomaly Detection	No	Some	Yes
Customization	Yes	Some	Yes

### Researcher Contact Information



Alfonso Valdes  
 valdes@cs1.sri.com  
 (650) 859-4976

### About SRI

SRI International (www.sri.com) is one of the world's leading independent research and technology development organizations. Founded in 1946 as Stanford Research Institute, SRI has been meeting the strategic needs of global markets for 60 years. As part of its strategy to bring its technologies to the marketplace, SRI licenses its technologies, forms strategic partnerships, and creates spin-off companies.

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

## Functional Description

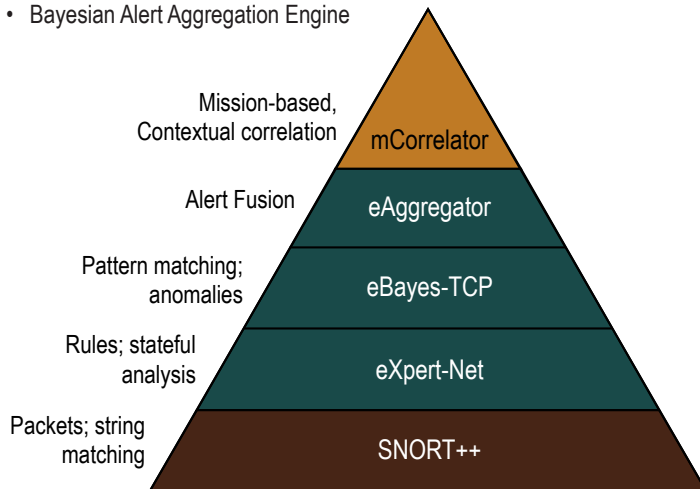
The EMERALD NetIDS Appliance is a turnkey appliance, providing high performance, ease of configuration and deployment, and security of the IDS system itself. The appliance operates as a passive (stealth) device and has two Ethernet interfaces, a read-only interface that only listens to traffic on the monitored network, and a second interface that connects to a private management network for configuration and alert messaging. Numerous EMERALD NetIDS Appliances can be deployed at various points of the network, and forward their alerts to a central database. Operators configure the appliance over the management network with any standard web browser supporting SSL.

## Technical Description

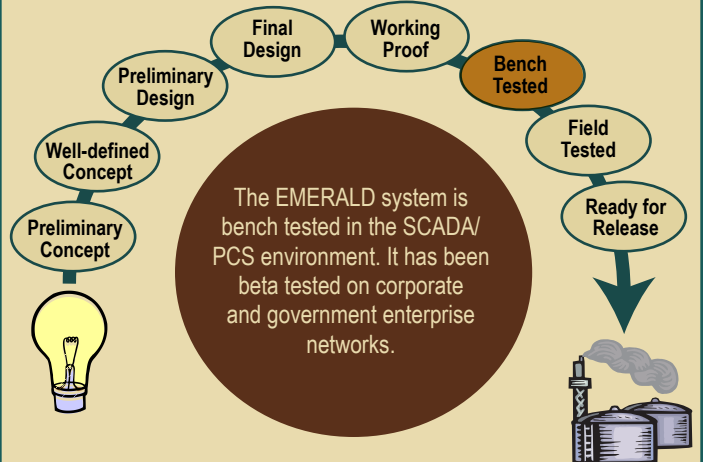
The EMERALD appliance includes a Postgresql database that stores network alerts and sensor status information. The Alert Management Interface (AMI) that provides the operator displays and reporting is Java-based, providing easy integration into a wide range of operating systems.

The Network IDS appliance includes the following features:

- Multi-algorithm, multi-level analysis
- SNORT incorporated in the EMERALD detection and correlation framework
- EMERALD Monitors Employed
- Stateful Packet Reassembly and Protocol Analysis Engine
- Stateless Packet Filtering Engine
- Bayesian Protocol Anomaly Detection Engine
- Bayesian Alert Aggregation Engine

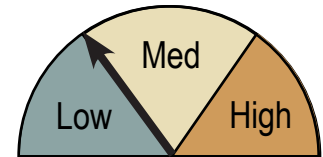


## Technology Transfer and Readiness



EMERALD detection and correlation component suite provides a cost effective detection and correlation solution for owner/operators of process control systems, with a knowledge base customized for the MODBUS protocol. It is available for pilot deployment in process control networks by arrangement with SRI International. Inquiries from control system and control system security vendors are welcome. All inquiries should be addressed to Douglas Bercow, Director of Business Development, SRI International ([douglas.bercow@sri.com](mailto:douglas.bercow@sri.com); 650-859-5187).

## Summary of Costs



	Low	Medium	High
<b>Component</b>	<\$1,000	\$1,000-\$10,000	>\$10,000
<b>Engineering</b>	Drop-in	Moderate modification	Complete System Design Lifecycle
<b>Bandwidth/Network Burden</b>	None-Passive Only	Moderate Traffic, Medium Overhead	Heavy Traffic, Large Overhead
<b>Training</b>	No training required	Moderate training	Intensive training. Additional staffing may be required.
<b>Maintenance and Operation</b>	< 1 hour per week	< 5 hours per week	> 5 hours per week