



*Das BSI zugelassene Sicherheitsgateway  
mit Informationsflusskontrolle*

**Sicherer Informationstransfer zwischen roten und schwarzen Domänen**

## Netzabgrenzung und Informationsflusskontrolle auf der F124

*Erfolgreiches Pilotprojekt für den Einsatz des von INFODAS und GeNUA entwickelten und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bis GEHEIM zugelassenen RSGate<sup>®</sup> (Rot/Schwarz-Gateway) auf einer Fregatte der Klasse F124*

Das von den Firmen INFODAS und GeNUA gemeinsam entwickelte Produkt **RSGate<sup>®</sup>** hat seine erste Einzelzulassung BSI-EZ-VSA-0001-2008. Die Zulassung ermöglicht einen Einsatz in allen Dienststellen der Marine (mobil und ortsfest). Das **RSGate<sup>®</sup>** stellt eine sichere Verbindung mit einer Informationsflusskontrolle sowohl zwischen nationalen Netzen als auch zu bestimmten internationalen und NATO-Netzen her.

**Motivation:** Bei der Arbeit mit Verschlusssachen unter dem Einsatz von Informationstechnik ist sicherzustellen, dass die Vorgaben des Geheimschutzes, insbesondere hinsichtlich des Schutzes vor unkontrollierter Weitergabe und Übertragung in einen niedriger eingestuften Bereich gewährleistet werden. Durch die zunehmende Vernetzung der Systeme geht die Bundeswehr – wie auch die wichtigsten Verbündeten – den Weg der Migration aller Informationssysteme in Richtung IP-basierter Kommunikation u. a. mit dem Ziel, zugelassene Verbindungen zwischen unterschiedlich eingestuften Sicherheitsdomänen zu schaffen. Dies insbesondere vor dem Hintergrund der Vernetzten Operationsführung (NetOpFü).

Die Marine konzipiert auf den neuen Schiffen wie bspw. den Korvetten K130 oder den Fregatten F125 sog. integrierte Bordnetze, an die alle Waffen- und Informationssysteme an Bord angeschlossen sind.

Die Informationen bei hochkomplexen modernen Waffensystemen – wie Sie auf den Schiffen zum Einsatz kommen – müssen unter betrieblichen und taktischen Gesichtspunkten zuverlässig getrennt werden. Bei der Aufklärung von See- und Luftzielen entstehen Daten in einem eingestuften Netz, die von Missions- und Supportsystemen verarbeitet werden müssen.

Letztlich ist selbst die Anbindung an weltweite öffentliche Netze für ein Kriegsschiff eine durchaus realistische Option, die mit der vorliegenden Lösung durchaus realistisch umgesetzt werden kann.



**Hintergrund:** Gemäß dem von der NATO definierten **Rot/Schwarz-Prinzip** müssen elektrische Leitungen, Bauteile, Geräte, Systeme, Netze usw. sicher voneinander getrennt werden. Dies betrifft zum einen eingestufte Informationen, die als Klartext in Form von Signalen verarbeitet oder übertragen werden (**Rot**) und zum anderen kryptierte oder als offen eingestufte Informationen (**Schwarz**). Während die Probleme des Zugriffs, der Bearbeitung oder der Durchleitung von roten Daten über schwarze Netze mittels VPN-Lösungen bzw. SINA-Technologie beherrscht werden, zeigt sich zunehmend die Notwendigkeit, Daten aus einem **roten** in ein schwarzes Netz hinein zu transferieren. Dabei sind die Daten inhaltlich zu kontrollieren und die Berechtigungen für den Transfer präzise und nachweisbar zu prüfen. Herkömmliche Firewall-Systeme filtern Daten lediglich hinsichtlich ihrer protokolltechnischen Eigenschaften wie Absender, Empfänger, verwendetem Kommunikationsprotokoll; eine inhaltliche Prüfung der übertragenen Daten wird jedoch nicht vorgenommen.

Es stellt sich also die Frage, wie eine **rote Sicherheitsdomäne** mit einer niedriger eingestuften **schwarzen Sicherheitsdomäne** verbunden werden kann und dabei eine kontrollierte sowie revisionssichere Kommunikation zwischen Systemen in beiden Sicherheitsdomänen ermöglicht wird.

### **Die Lösung und ihre Funktionalitäten:**

Die im Rahmen einer Studie für die Fregatten der Klasse F125 konzipierten Lösungsprinzipien der Informationsflusskontrolle mittels **RSGate**<sup>®</sup> wurden in einem Truppenversuch an Bord einer Fregatte der Klasse F124 von INFODAS integriert. Damit wurde erfolgreich nachgewiesen, dass ein Informationsfluss auch unter Einsatz- und Lastbedingungen zuverlässig, performant und benutzerfreundlich zu steuern und zu kontrollieren ist. Der Leistungsumfang des modular aufgebauten **RSGate**<sup>®</sup> an Bord umfasst:

- die automatische Prüfung von Statusmeldungen und Sensordaten, die zwischen der operativen Einsatz-Software CDS (**rotes Combat Direction System**) und der Automationsanlage IMCS (**schwarzes Integrated Monitoring and Control System**) ausgetauscht werden,
- die exakte Prüfung der zu übertragenden Daten gegen ein im Sicherheitsfilter hinterlegtes und konfigurierbares Regelwerk („byte-genau“) sowie die damit kontrollierte Weiterleitung der Daten,
- die manuelle Freigabe von E-Mails (Dateiübertragung als E-Mail-Anhänge (SMTP)) eines Benutzers in einer **roten Sicherheitsdomäne** an einen Empfänger in einer **schwarzen Sicherheitsdomäne**, zum einen durch eine vertrauenswürdige Darstellung („what you see is what you sign“-Prinzip) und zum anderen auf die Abgrenzung unterstützter Dateiformate wie TXT, ADatP-3, BMP oder RTF,
- den Schutz vor Angriffen aus dem **schwarzen Netz** durch eine integrierte Firewallfunktionalität,
- die Verifikation der angebrachten Signaturen mittels des zentralen Sicherheitsfilters sowie die integrierten Funktionen zur sicheren Administration der Komponenten.

Bei der Komplexität der zu lösenden Aufgabe erfreut die Aussage des Führungssystem-Offiziers der Fregatte HESSEN: „das eingesetzte **RSGate**<sup>®</sup> funktioniert einwandfrei und stört den Betrieb nicht“.

INFODAS GmbH sieht in einer solchen Kundenzufriedenheit die Bestätigung ihrer praxisnahen und einsatzunterstützenden Lösung.

---

### **Über die INFODAS GmbH**

INFODAS gehört zu den innovativen deutschen mittelständischen Systemhäusern für IT-Sicherheits- und Risikomanagement. Neben Konzeption, Entwicklung, Integration und Aufbau von evaluierten IT-Sicherheitslösungen führen die von BSI-lizenzierten ISO 27001- und IT-Grundsicherheits-Auditoren geleiteten Projektteams der INFODAS ganzheitliche IT-Sicherheitsberatungen mit Hilfe des Werkzeugs **SAVe**<sup>®</sup> durch. Sie konzipieren bzw. auditieren IT-Sicherheitsmanagementsysteme gemäß ISO 27001, BSI-Standard 100-1 bzw. ZDv 54/100. INFODAS entwickelt geeignete Notfallvorsorge-Programme, gestaltet und überprüft den Datenschutz und stellt externe Datenschutzbeauftragte zur Verfügung.