

Erhöhte Sicherheit für Kreuzfahrtschiffe durch integriertes Netzwerk

*Jens Prüfer**

The Term "Service Integrated Network" stands for one unified global network for all data services aboard maritime vessels. It can be shown that such a network is more secure than conventional solutions deploying separate networks with respect to both - operational reliability as well as resilience against abuse by malicious users (hackers). Utilising the monitoring capabilities of the active components a significant increase in safe operations of all connected services is achieved. At the same time cabling costs as well as expenses for maintenance are cut and the availability of ship data is increased, thus developing new sources of revenue for the ships owner.

Das "Service Integrated Network" ist ein einheitliches, umfassendes Netzwerk für alle Dienste an Bord von Schiffen. Es kann gezeigt werden, dass ein solches Netzwerk mehr Sicherheit als konventionelle Lösungen bietet – sowohl unter dem Aspekt der Betriebssicherheit als auch bei der Abwehr böswilliger Nutzer. Durch aktive Komponenten lässt sich das Netzwerk einfacher überwachen. Dies erhöht die Betriebssicherheit für alle Dienste. Gleichzeitig wird der Verkabelungs- und Instandhaltungsaufwand geringer – und damit die Verfügbarkeit aller Schiffsdaten erhöht. Dies bringt dem Schiffseigner klare Kostenvorteile.

Bisher wird an Bord von Schiffen eine große Zahl separater Netzwerke für die unterschiedlichen Dienste verlegt und gewartet. Standardisierte Schnittstellen fehlen, so dass ein Austausch der Informationen zwischen den Systemen - z.B. für die Einführung eines Voyage Data Recorders die Ingenieure immer wieder vor eine schwierige Aufgabe stellt. Teilweise werden die Daten sogar noch per Ausdruck und Handeingabe übertragen.

Im Service Integrated Network sollen zunächst alle nicht sicherheitskritischen Dienste und Services wie Passagierinformationssystem, Telefone und Unterhaltungsmedien in einem Netzwerk integriert werden. Langfristig jedoch sollen auch Alarmsysteme und Automation über das gemeinsame Netzwerk kommunizieren und für den Informationsaustausch einheitliche Schnittstellen zur Verfügung stellen.

Die Vorteile liegen auf der Hand. Eine einheitliche Infrastruktur sorgt für reduzierten Verkabelungsaufwand, geringere Anschaffungs- und Betriebskosten, vereinfachte Wartung und nicht zuletzt für eine bessere Verfügbarkeit der übertragenen Informationen. Durch die jetzt zur Verfügung stehenden Daten kann die Effizienz des Schiffsmanagements erheblich verbessert werden. Auf Passagierschiffen können völlig neue Service- Angebote genutzt werden. Die Verwendung modernster Glasfasertechnik stellt sicher, dass auch bei eventuellem Retrofitting die Verkabelung nicht angetastet werden muss.

Will man sicherheitsrelevante Daten über ein Netzwerk transportieren, so kommen sofort Fragen nach der Sicherheit des Übertragungssystems auf. Es gilt hier prinzipiell zwei Arten von Sicherheit zu unterscheiden. Erstens die reine Betriebssicherheit der Systeme gegen Ausfälle und technische Störungen. Andererseits die Sicherheit vor böswilligen Nutzern, die sich ein solches Netzwerk für unerlaubten Datenzugriff oder schlimmstenfalls Sabotage zunutze machen könnten.

Die Furcht vor letzterem ist seit der öffentlichen Diskussion um Virenbefall, Hintertüren und Trojanische Pferde in den Medien stetig größer geworden.

Betriebssicherheit

Vielfach hört man das Argument, ein einzelnes Netzwerk sei für den gemeinsamen Betrieb von sicherheitsunkritischen und kritischen Diensten zu unsicher. Schließlich könne ein Totalausfall aller Systeme auf einmal durch den Defekt in nur einem Übertragungsnetzwerk drohen. Daher werden von den Werften und Klassen bisher unterschiedliche Netzwerke für die verschiedenen Gewerke verlegt und teilweise gefordert.

Ob dadurch ein Sicherheitsgewinn erzielt werden kann, ist fragwürdig. Angenommen, ein Netzwerk hat eine unabhängige, konstante Ausfallwahrscheinlichkeit. Dann haben n unabhängige Netzwerke auch die n -fache Ausfallwahrscheinlichkeit. Die Wahrscheinlichkeit, dass ein einzelnes Netzwerk ausfällt, wird nicht verkleinert und die Wahrscheinlichkeit überhaupt einen Defekt an Bord zu bekommen, steigt sogar. Lediglich die Wahrscheinlichkeit für einen Totalausfall aller Systeme wird stark reduziert.

Nur durch die Einführung von redundanten Netzwerken kann die Ausfallwahrscheinlichkeit für einzelne Gewerke gesenkt werden. Die Wartung vieler unterschiedlicher Netzwerke ist aber eine komplexe und zeitraubende Angelegenheit. Will man die Sicherheit für alle Systeme gleichermaßen erhöhen, so wird dies durch ein gemeinsames, redundant ausgelegtes Netzwerk einfacher erreicht. Die Wahrscheinlichkeit für einen Ausfall einzelner Systeme durch Defekte im Übertragungsnetzwerk wird durch einfache Redundanz erheblich gesenkt. Ist also für gemeinsames Netzwerk von der technischen Seite auf die gleichzeitige Übertragung aller Daten ausgelegt und sauber konfiguriert, wird durch das Verlegen weiterer Netzwerke kein Sicherheitsgewinn erzielt.

Seit der Einführung des CSMA/CD-Verfahrens in Xerox „Ethernet“ hat sich in der Entwicklung der Netzwerktechnik sehr viel getan. Die zur Verfügung stehende Bandbreite wurde um mehr als einen Faktor 1000 erhöht. Im Gegenzug werden für die Datenübertragung durch Einführung ausgeklügelter Kompressionsalgorithmen immer geringere Bandbreiten benötigt. So kann heute eine PAL Videoübertragung, die in Rohfassung bis zu 270 MBit/sec benötigt, dank MPEG2 Codierung in bester DVD Qualität bei maximal 3 Mbit/sec durchgeführt werden.

Durch Priorisierung der Daten und Bandbreitenmanagement - den sogenannten QoS Merkmalen - die im IPv6 Protokoll besonders unterstützt werden, ist außerdem gewährleistet, dass die vom Volumen zwar geringen, aber extrem wichtigen Steuer- und Sensordaten ohne Verzögerung weitertransportiert werden. Durch die redundante Auslegung des Netzwerkes ist die Betriebssicherheit zu allen Zeiten gewährleistet, ein Totalausfall ist praktisch ausgeschlossen.

Ein weiterer Vorteil des Service Integrated Networks ist, dass ein proaktives Fehlermanagement Probleme z.B. durch defekte Netzwerkschnittstellen oder Fehlkonfiguration bereits vor einem Totalausfall erkennen und melden kann. Sollte beispielsweise ein defektes Netzwerkinterface permanent Kollisionen und damit sehr hohen Datenverkehr erzeugen, wird dieses von der Netzwerküberwachung sofort erkannt und mit Angabe des genauen Standortes und des befallenen Interfaces gemeldet. Die Schnittstelle kann schnell und einfach ausgetauscht werden. Bis dahin wird sie automatisch vom Netz getrennt um ein „flooding“ des Netzwerkes zu verhindern.

Auch eine Ferndiagnose per Satellitenkommunikation wird vereinfacht. So können ggf. benötigte Ersatzteile am nächsten Hafen vorgehalten werden, teure Ausfallzeiten werden minimiert.

Sicherheit gegen böswillige Nutzer

Gerade die Anbindung an das Internet wirft aber eine weitere Frage auf: Wie sicher ist ein solches Netzwerk gegen böswillige Angriffe von außen? Der Film „Speed2 - Cruise Control“ zeigt ein solches Horrorszenario, in dem ein an Bord befindlicher Passagier mit kriminellen Absichten bequem von seiner Kabine aus die Kontrolle über ein ganzes Kreuzfahrtschiff übernimmt. Schaut man sich den Film genauer an, merkt man aber sofort, dass hier nur maßlose Hollywood-Übertreibung gezeigt wird.

Natürlich gilt auch für ein modernes Kommunikationsnetzwerk: Die Kette ist nur so stark wie das schwächste Glied. Es ist notwendig, den physikalischen Zugang zu sensiblen Bereichen, wie Brücke, Maschinenraum und anderen technischen Einrichtungen für Unbefugte zu verhindern. Nur dann machen weitere Sicherheitsmaßnahmen überhaupt einen Sinn.

Durch die Einteilung des Netzwerkes in VLAN Gruppen (Virtual LAN) wird das physikalische Netzwerk in unabhängige logische Netzwerke unterteilt. Das führt zu einer Entflechtung des Datenverkehrs und verhindert, dass sensible oder betriebswichtige Daten überhaupt in den Passagierbereich gelangen. Alle Zugangsterminals können mit konventioneller und biometrischer Zugangskontrolle ausgestattet werden. Auf diese Weise wird erreicht, dass auf Nutzerebene nur bestimmte Daten zur Verfügung gestellt werden und der Einblick in sensible Bereiche verwehrt bleibt. So ist es möglich, dass prinzipiell alle Informationen an den jeweiligen Bedienstationen der Crew, nicht jedoch an denen der Passagiere zur Verfügung stehen. Bei einer Alarmmeldung kann ein Ingenieur sich einfach per Chipkarte oder Fingerabdruck am nächsten Terminal identifizieren und erhält sofort alle verfügbaren Informationen über die Störung, egal wo auf dem Schiff, er sich gerade befindet.

Der Zugang aus dem Internet zum Schiff wird durch Firewalls vor unbefugten Zugriffen geschützt. Intrusion Detection Systeme überwachen zusätzlich das Netzwerk, um bei Manipulationen an Daten Alarm zu geben. Damit ein Abhören sensibler Daten durch Dritte auf dem Übertragungswege sicher unterbunden werden kann, wird eine starke Verschlüsselung der Daten durchgeführt.

Fazit

Hundertprozentige Sicherheit wird es niemals geben. Das Service Integrated Network ist aber den konventionellen Systemen in Puncto Sicherheit überlegen. Dank der durchgängig aktiven Komponenten ist ein stark verbessertes Fehlermanagement möglich, das bei konventionellen Systemen in der Weise nicht verfügbar ist. Betrachtet man den hohen zusätzlichen Kundennutzen und die einfache Erweiterbarkeit, ist das Service Integrated Network eine sinnvolle und sichere Investition auf höchstem technischen Niveau.

*Jens Prüfer, Siemens AG, Marine Solutions, Hamburg

Bild 1: Service Integrated Network - One for All

Bild 2: Höchste Ausfallsicherheit durch Redundanz

Erschienen in „Schiff & Hafen“, Seehafen Verlag, Hamburg, Nr.6 Juni 2002, S.11-14

Leseranfragen bitte unter dem Stichwort „I&S 0302.2743“ an:

Siemens AG, I&S GC P, Dr. Rainer Schulze, D-91050 Erlangen,

Tel.: 09131-7-44544, Fax: 09131-7-25074

E-Mail: rainer.schulze@siemens.com