FernUniversität in Hagen,
Fakultät für Mathematik und Informatik
Lehrgebiet Rechnerarchitektur

Univ.-Prof. Dr. Wolfram Schiffmann

Masterarbeit im Fach Praktische Informatik

Anwendung und Untersuchung einer Methode zur Analyse von IT-Sicherheitsrisiken anhand eines hochwertigen Erdfernerkundungssystems

(SS 16)

Silke Kerkhoff

Matrikelnummer: 7499221

Erstgutachter: Prof. Dr. W. Schiffmann

Betreuer und Zweitgutachter: Dr. Jörn Eichler

Fraunhofer AISEC

Inhaltsverzeichnis

Kurzfassung

Die vorliegende Masterarbeit gibt einen Überblick über die Anwendung und Untersuchung einer Methode zur Analyse von IT-Sicherheitsrisiken anhand eines hochwertigen Erdfernerkundungssystems. Die Threat, Vulnerability and Risk Analysis (TVRA)-Methode wurde auf das hochwertige Erdfernerkundungssystem angewendet und dabei näher betrachtet, sowie mit einer Risikoanalyse nach IT-Grundschutz verglichen. Die Methode bietet eine umfassende Möglichkeit an, um die Sicherheitsrisiken, die bekämpft werden müssen, zu identifizieren. Bei der Anwendung der Methode wird Fachwissen und eine manuelle Auswahl benötigt. Dadurch erhalten die Ergebnisse der Analyse eine subjektive Bewertung. Die TVRA-Methode ist für die Risikoanalyse eines hochwertigen Erdfernerkundungssystems systematisch anwendbar. Durch spezifische Anpassungen der Methode an den Anwendungsfall, können zusätzliche Sicherheitsprobleme des hochwertigen Erdfernerkundungssystems erkannt werden.

Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich bei der Anfertigung dieser Masterarbeit begleitet haben. Ganz besonders möchte ich meinem Betreuer Herrn Dr. Jörn Eichler danken, der mich im Rahmen der Masterarbeit betreut hat und mir jederzeit mit Rat und Tat zur Seite stand.

Auch gilt mein Dank vielen meiner Kollegen, die mir während der Anfertigung dieser Abschlussarbeit in meiner Arbeitsgruppe den Rücken frei gehalten haben, die ich zu jeder Zeit um Rat fragen konnte und die mich immer unterstützen.

Nicht zuletzt möchte ich mich bei meinen Eltern bedanken, die mich bei dieser Arbeit und während meines Studiums unterstützt haben.

Mein besonderer Dank gilt meinem Freund Robert, der mich mit viel Geduld moralisch und durch seine fachliche und persönliche Unterstützung durch das Studium und diese Arbeit begleitet hat.

Abbildungsverzeichnis

Tabellenverzeichnis

Liste der Abkürzungen

ALE	Annualized Loss Expectancy
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CoSSC	Coregistered Single look Slant range Complex
DAS	Direct Archive System
DEM	Digital Elevation Model
DFD, DLR-DFD	Deutsches Fernerkundungsdatenzentrum
DIMS	Data and Information Management System
DIN	Deutsches Institut der Normung e.V.
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DMZ	Demilitarisierte Zone
EAL	Evaluation Assurance Level
EOC, DLR-EOC	Earth Observation Center
ETA	Ereignisbaumanalyse
ETSI	Europäisches Institut für Telekommunikationsnormen
EVG	Evaluationsgegenstand
FMEA	Failure Mode and Effects Analysis
FTA	Fehlerbaumanalyse
FTPS	File Transfer Protocol über SSL oder TSL
GS	Ground Segment
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
INU	Bodenstation Inuvik/Kanada
IOCS	Instrument Operations and Calibration Segment
IT	Informationstechnologie
ITP	Integrated TanDEM Processor
KMF	Key Management Facility
LAN	Local Area Network
MF, DLR-MF	Institut für Methodik der Fernerkundung
MOS	Mission Operations Segment
MPI	Mission Planning Interface

MPS	Mission Planning System
NSG	Neustrelitz Ground Station
NZ	Neustrelitz
OC	Ordering Control
OP	Oberpfaffenhofen
OWASP	Open Web Application Security Project
PAF	Processing and Archiving Facility
PC	Production Control
PGS	Payload Ground Segment
PI	Principle Investigator
PL	Product Library
PMT	Production Management Team
PP	Protection Profile
RAID	Redundant Array of Independent Disks
RS-NSG	Receiving Station Neustrelitz
R2CC	Request to Command-Converter
RZ	Rechenzentrum
SAM-FS	Storage and Archive Manager Filesystem
SAN	Storage Area Network
SAR	Synthetic Aperture Radar
SAR (bei CC)	Security Assurance Requirement
SatDSiG	Satellitendatensicherheitsgesetz
SF	Security Function
SFR	Security Function Requirement
sftp	Secure File Transfer Protocol
SOL	Single Occurrence Losses
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TDM	Mission TanDEM-X
TDX	Tandem-X-Satellit
TMSP	TerraSAR Multimode SAR Processor
TOE	Target of Evaluation (siehe auch EVG)
TSC	Transcription Processing System
TSF	TOE Security Functionality
TSL	Transport Layer Security

TSM	Mission TerraSAR-X
TSX	TerraSAR-X-Satellit
VPN	Virtual Private Network
XML	Extensible Markup Language

1 Einleitung

In der Einleitung wird in das Thema der Masterarbeit eingeführt, sowie die Motivation und Fragestellung dargestellt. Im Abschnitt 1.2 wird eine Abgrenzung und Einordnung dieser Masterarbeit in die Themengebiete der Informatik gegeben. Der Abschnitt 1.3 beschreibt die Vorgehensweise und den Aufbau der Arbeit.

1.1 Motivation und Fragestellung

IT-Systeme sind zur heutigen Zeit ein zentraler Bestandteil unseres Lebens. Diese IT-Systeme werden immer komplexer und dadurch auch immer leichter angreifbar. Die Entwicklung sicherer Software und sicherer Systeme ist mittlerweile häufig eine Anforderung der Kunden und auch eine wirtschaftliche und rechtliche Notwendigkeit vieler Unternehmen. Die Daten der Unternehmen werden digital erfasst, verarbeitet und gespeichert. Bei Diebstahl oder Manipulation der Daten kann dies unter Umständen zu finanziellen, juristischen oder gar Personenschäden führen.

In dem jährlichen Sicherheitsreport 2015 von Cisco Systems Inc. [Abbildung 1-1 Monatlich gesammelte akkumulierte Störmeldungen der Jahre 2012 bis 2014 [Ci15] ist zu erkennen, dass im November 2014 die Gesamtzahl der über das Jahr akkumulierten Störmeldungen geringer war, als im Jahr zuvor.

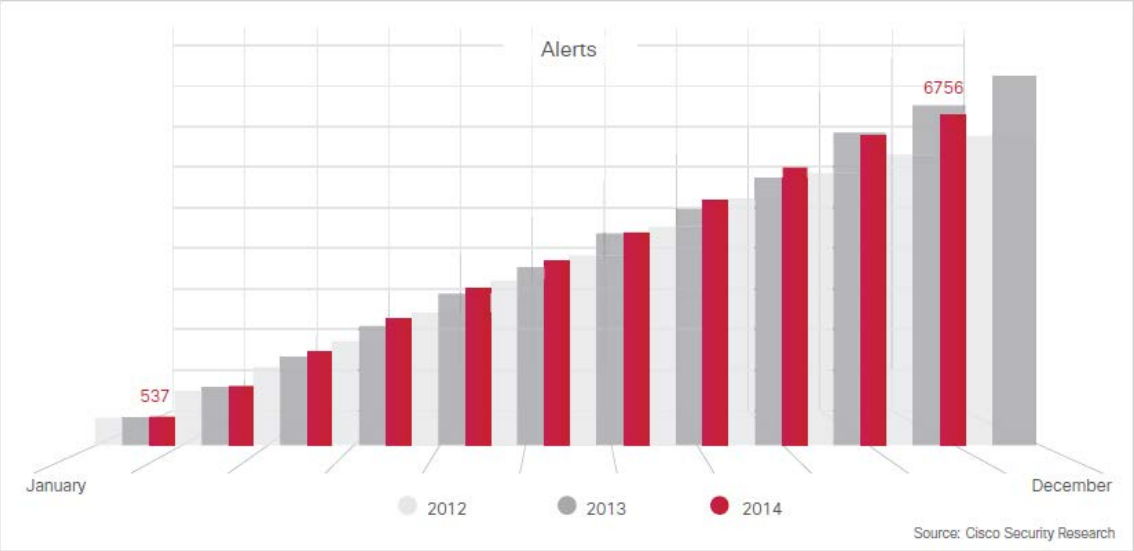

Abbildung 1-1 Monatlich gesammelte akkumulierte Störmeldungen der Jahre 2012 bis 2014 [Ci15]

Der Anteil von 1,8 % erscheint zwar klein, aber es ist das erste Mal, dass die Anzahl der Warnungen gegenüber dem Vorjahr gesunken ist.

Der wahrscheinlichste Grund dafür liegt in der größer werdenden Aufmerksamkeit beim Testen der Software und der Entwicklung auf Seiten der Hersteller. Verbesserte Lebenszyklen bei der Entwicklung reduzieren die Sicherheitslücken, die von Angreifern genutzt werden können [Ci15].

Nicht zuletzt spiegelt der Report auch die Relevanz des Themas sicherer IT-Systeme in unserer Gesellschaft wieder. „Die Qualität eines sicheren IT-Systems hängt wesentlich davon ab, dass seine Konstruktion methodisch und systematisch erfolgt“ [Ec14, Vorwort].

In Deutschland entstehen hochwertige Erdfernerkundungssysteme, die Daten mit sehr hohem Schutzbedarf erzeugen, mit dem Ziel einer weltweiten gewerblichen Vermarktung. Im Juni 2007 wurde der räumlich hochauflösende Radarsatellit TerraSAR-X gestartet, dem 2010 sein Zwillingssatellit TanDEM-X folgte. Bei der TerraSAR-X- und TanDEM-X-Mission werden beide Satelliten in Formation betrieben, um hochauflösende Radarbilder und digitale Geländemodelle der Erdoberfläche zu erzeugen.

Die Mission liefert hochwertige Erdfernerkundungsdaten, die zur weltweiten zivilen Vermarktung zur Verfügung stehen. Bis dato wurden solch qualitativ hochwertige Daten nur für militärische Zwecke verwendet. Da das Verbreiten dieser Daten mit hohem Informationsgehalt die sicherheitspolitischen Interessen der Bundesrepublik Deutschland gefährden kann, findet das Satellitendatensicherheitsgesetz, im folgenden SatDSiG genannt, beim Umgang mit diesen Daten Anwendung. Am 20. September 2007 wurde das Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (SatDSiG) verabschiedet und trat am 01. Dezember 2007 in Kraft [BMW08].

Eine wesentliche Aufgabe des SatDSiG ist es, den Betrieb hochwertiger Erdfernerkundungssysteme und die Verteilung der damit gewonnenen Daten zu reglementieren, um ein sicheres System für die Aufnahme, Generierung, Speicherung und Verbreitung der Daten aufzubauen. Ein solches System ist unterschiedlichen Bedrohungen ausgesetzt, die bereits bei dessen Entwicklung und Konstruktion berücksichtigt werden müssen.

Die Anforderung an Behörden und Unternehmen, dass sie den Nachweis erbringen, ausreichend für Informationssicherheit vorzusorgen, steigt zunehmend an. Durch den Einsatz von anerkannten Standards und Normen innerhalb der Behörde oder des

Unternehmens kann auf bewährte Vorgehensweisen zurückgegriffen werden. Die Standards orientieren sich am Stand von Technik und Wissenschaft, gewährleisten Aktualität und stärken die Rechtssicherheit [BD07, S. 8].

Ein gängiges Verfahren zur Bewertung von Sicherheitsrisiken ist die Risikoanalyse. Mit der Risikoanalyse werden die Risiken identifiziert, bewertet und der potentielle Schaden, sowie die Wahrscheinlichkeit für das Eintreten des Schadensfalls abgeschätzt. Als Ergebnis werden effektive Maßnahmen geplant und die identifizierten Risiken laufend überwacht.

Das Europäische Institut für Telekommunikationsnormen (ETSI) ist eine anerkannte Organisation, die europaweit Standards, Normen und Spezifikationen im Bereich der Telekommunikation erarbeitet [BNA15]. Ziel der Arbeit ist es, festzustellen, ob die Anwendung der ETSI-Standardmethode Threat, Vulnerability and Risk Analysis (TVRA) [ETS11] für den Aufbau eines hochwertigen Erdfernerkundungssystems im Zusammenhang mit dem SatDSiG [BJV07] geeignet ist. Die TVRA ist eine Methode, um Risiken der IT-Sicherheit zu bewerten. Sie wird in der technischen Spezifikation TS 102 165-1 [ETS11] beschrieben und bietet eine strukturierte und systematische Vorgehensweise, um potentielle Risiken basierend auf der Wahrscheinlichkeit eines Angriffs und die Auswirkungen, die ein solcher Angriff auf das System haben kann, zu identifizieren. Aus dieser Bedrohungs-, Schwachstellen- und Risikoanalyse werden zusätzliche sicherheitsrelevante Anforderungen abgeleitet.

Die TVRA richtet sich nach den Common Criteria for Information Technology Security Evaluation (CC). Die CC wurden im internationalen Standard ISO/IEC 15408 veröffentlicht und sind die gemeinsamen Kriterien nahezu aller informationstechnischen Produkte und Systeme für die Prüfung und Bewertung der Sicherheit von Informationstechnik [BSI06]. Die Anlehnung an die CC lässt vermuten, dass die TVRA für die Risikoanalyse bei dem Aufbau eines hochwertigen Erdfernerkundungssystems geeignet ist.

Durch ihre Anwendung für die Risikoanalyse soll der mögliche Mehrwert und die Anwendbarkeit der Nutzung einer standardisierten Methode identifiziert werden. So können ggf. Schwachstellen beim Aufbau eines hochwertigen Erdfernerkundungssystems erkannt werden, die vorher bei der Nutzung einer anderen Risikoanalysemethode nicht erkannt wurden, oder es können sich Alternativen für das Design aus der Methode ergeben. Die Verwendung der TVRA kann möglicherweise

auch zu Nachteilen führen, die im Rahmen der Masterarbeit ebenfalls beschrieben werden sollen.

1.2 Einordnung und Abgrenzung des Themengebietes

Die Arbeit gliedert sich in den Bereich Security Engineering ein. Security Engineering ist eine sich entwickelnde Disziplin, die aus den Bereichen Systems Engineering und Informationssicherheit (vgl. Kap. Informationssicherheit 2.3) besteht. Durch Hinzunahme des Aspektes Sicherheit entwickelt sich die Disziplin Security Engineering (siehe Kap. 2.4). Security Engineering behandelt Werkzeuge, Prozesse und Methoden für Entwurf, Implementierung und Tests von sicheren IT-Systemen [An01, S. 3].

Systems Engineering und Software Engineering sollte nicht verwechselt werden, obwohl sie viel gemeinsam haben. Software Engineering ist ein Fachgebiet, welches sich mit der Entwicklung von Software beschäftigt. Darüber hinaus unterstützt es durch die systematische Verwendung von Methoden, Werkzeugen und Prinzipien die Entwicklung von komplexer Software. Beim Systems Engineering werden ebenfalls Softwarekomponenten entwickelt, der Zweck des Systems Engineerings besteht jedoch darin, den Überblick über ein Projekt zu erhalten bzw. zu bewahren. Durch den Einsatz von unternehmensinternen, nationalen sowie internationalen Standards wird ein einheitlicher Systems Engineering Prozess unterstützt. Das Augenmerk bei dieser Arbeit liegt auf der Verwendung einer Risikoanalysemethode, um bereits beim Aufbau eines Erdfernerkundungssystems Schwachstellen zu identifizieren, welche im Fall von Angriffen auf das System genutzt werden könnten. Des Weiteren werden Vorkehrungen getroffen, um den erkannten Bedrohungen entgegen zu wirken und ein möglichst sicheres System aufzubauen.

An dieser Stelle soll darauf hingewiesen werden, dass sich diese Arbeit nicht mit sicherem Programmieren beschäftigt, welches auch ein Teilgebiet des Security Engineering ist.

Ferner wird in dieser Arbeit, wenn von Sicherheit die Rede ist, immer im Sinne von Security und nicht von Safety gesprochen (siehe Kapitel 2.3 für den Unterschied von Safety und Security).

Da aufgrund ihrer großen Anzahl nicht alle Risiken und Sicherheitsanforderungen für das gesamte System detailliert abgeleitet werden können, werden in dieser Arbeit

diejenigen Risiken und Sicherheitsanforderungen behandelt, die sich aus dem SatDSiG ergeben. Hierbei werden nur einige Teilgebiete des Systems betrachtet, um den Umfang der Arbeit einzugrenzen.

1.3 Vorgehensweise und Aufbau der Arbeit

In diesem Abschnitt werden der Aufbau und die Vorgehensweise der Arbeit beschrieben. Des Weiteren wird ein Überblick über die Inhalte der einzelnen Kapitel gegeben.

Im folgenden Kapitel 2 werden die Grundlagen, Definitionen und Begriffe, die in der Arbeit verwendet werden, anhand von geeigneter Fachliteratur und Internetrecherchen aufgeführt. Dadurch wird dem Leser ein gemeinsames Verständnis über die wichtigsten Begriffe gegeben, die für die darauffolgenden Kapitel benötigt werden.

Zunächst werden die Elemente eines hochwertigen Erdfernerkundungssystems incl. Sicherheitsanforderungen, die sich nach SatDSiG ergeben, identifiziert. Anschließend werden die Begriffe der Informationssicherheit, ihren Schutzzielen und dem Security Engineering erläutert. Abgeschlossen wird das Kapitel 2 mit den Grundlagen einer Risikoanalyse, sowie deren Bedrohungskategorien und der Bewertung und Behandlung von Risiken. Das letzte Unterkapitel umfasst die Grundlagen und notwendigen Begriffe der Common Criteria.

Kapitel 3 beginnt mit einem Überblick über eine Auswahl vorhandener Risikoanalysemethode im Bereich Informationssicherheit. Mit der Beschreibung der Risikoanalyse auf der Basis von IT-Grundschutz, die bei der TanDEM-X-Mission verwendet wurde, wird das Kapitel 3 weitergeführt. Die Risikoanalyse auf der Basis von IT-Grundschutz wird später zum Vergleich herangezogen. Gefolgt wird diese Beschreibung von den theoretischen Grundlagen der TVRA-Methode. Anschließend wird die TVRA-Methode an hochwertige Erdfernerkundungssysteme für die Teilgebiete Bodenstation, Transkription Prozessierungssystem und einer Webschnittstelle zur Suche, Bestellung und Auslieferung von Erdfernerkundungsdaten angewendet. Durch die Anwendung der Methode sollen Erkenntnisse erlangt werden, ob Sicherheitsexperten und Entwickler bei der Bewertung von Risiken und Schwachstellen im Design durch diese Methode im Einsatz bei einem hochwertigen Erdfernerkundungssystem unterstützt werden. Diese Untersuchung findet im Anschluss, im Kapitel 4, statt.

In Kapitel 5 werden die Ergebnisse der Risikoanalyse beschrieben und die Methode anhand von vorher festgelegten Bewertungskriterien bewertet und mit Ergebnissen aus der Risikoanalyse auf der Basis von IT-Grundschutz verglichen. Anschließend folgt eine Diskussion der Ergebnisse und Empfehlungen für die Anpassung dieser Methode an diverse Anwendungen auf ein hochwertiges Erdfernerkundungssystem.

Im abschließenden Kapitel 6 werden die Ergebnisse der Arbeit reflektiert und weitere mögliche Einsatzgebiete der TVRA-Methode genannt, bevor ein Gesamtfazit gezogen wird.

2 Grundlagen

Zu Beginn dieses Kapitels werden Grundlagen eines Erdfernerkundungssystems (siehe 2.1) und Definitionen aus dem Gesetzestext des SatDSiG (2.2) aufgeführt, welche im weiteren Verlauf der Arbeit benötigt werden. Des Weiteren werden in diesem Kapitel die zum Verständnis dieser Arbeit notwendigen Grundlagen ermittelt. Es werden Begriffsdefinitionen aus gängiger Fachliteratur aus den Bereichen IT-Sicherheit (siehe 2.3), Security Engineering (2.4) und im speziellen der Risikoanalyse eingeführt. Zum Abschluss dieses Kapitels werden noch die Common Criteria/Common Methodology näher erläutert. Dies dient unter anderem dazu, eine einheitliche Terminologie der verwendeten Begriffe und ein einheitliches Verständnis des Themenkomplexes zu schaffen.

2.1 Erdfernerkundungssystem

Ein Erdfernerkundungssystem setzt sich aus verschiedenen Teilsystemen zusammen. Die relevantesten sind nachfolgend kurz erläutert.

Erdbeobachtungssatellit

Ein Satellit ist ein Weltraumkörper, der einen Himmelskörper umkreist. Ein Erdbeobachtungssatellit wird zur laufenden Messung und systematischen Aufzeichnung von Sachverhalten der Erdoberfläche verwendet. Die Vorteile von Erdbeobachtungssatelliten liegen in ihrer hohen Wiederholrate, ihren aktuellen Daten und ihrer großen Gebietsabdeckung. Ihr Einsatzbereich ist weit gefächert. Sie werden u.a. in der Klimaforschung, der Meeres- und Gewässerkunde, der Geologie, der Kartographie und der Land- und Forstwirtschaft eingesetzt. Unterschieden werden Erdbeobachtungsatelliten nach Flughöhe, Umlaufbahn (Orbit), Sensoren, sowie ihrem Einsatz- und Aufnahmebereich. Sie verfügen im Vergleich zu Wettersatelliten über Instrumente mit einer höheren Auflösung. Die Sensoren werden in passive und aktive Sensoren unterteilt. Aktive Sensoren senden aktiv zum Objekt Strahlungen aus und messen den Anteil der Strahlung, die zum Sensor zurückgeliefert wird. Passive Sensoren messen entweder die vom Objekt selbst ausgesendete oder von dem Objekt reflektierte Strahlung. [Ba01]

In dieser Arbeit werden Satelliten mit aktuell sehr hoher Auflösung betrachtet. Dies können zum einen optische Satelliten mit panchromatischen oder multispektralen

Sensoren, wie zum Beispiel bei Ikonos oder WorldView, und zum anderen Radarsatelliten wie TanDEM-X sein.

Da in der Arbeit Radarsatelliten betrachtet werden, wird der Radarsatellit näher erläutert.

Radarsatelliten im herkömmlichen Sinne arbeiten nach dem Prinzip des Synthetischen Apertur Radars (SAR). Hierbei wird die Erde mit einem Strahl kohärenter Mikrowellenstrahlung, wie bei einem Laser, beleuchtet. Das Radar sendet Mikrowellenpulse aus, die von der Erdoberfläche reflektiert werden, um dann wieder von dem Radar empfangen zu werden. Der Abstand des Satelliten zur Erdoberfläche ergibt sich aus der Laufzeit der Signale. Das Radar zeichnet die Signale sequentiell auf und beleuchtet einen Streifen am Boden, da sich der Satellit um die Erde bewegt. Die Echo-Signale enthalten auch Informationen über die Oberflächenbeschaffenheit. Nach einer aufwendigen Signalverarbeitung entsteht ein zweidimensionales Bild des Gebietes. Mit Radar wird in einem Wellenlängenbereich gearbeitet, in dem die Strahlen ungehindert Nebel, Wolken oder Regen durchdringen. Radarsysteme beleuchten die Erdoberfläche aktiv, so dass sie unabhängig von der Tageszeit eingesetzt werden können. Diese beiden Eigenschaften machen den Einsatz von Radar zeit- und wetterunabhängig. [DLR01]

Empfangsstation

Die vom Satelliten kontinuierlich aufgenommenen Daten müssen auf der Erde empfangen und verarbeitet werden. Für den Empfang der Daten stehen weltweit mehrere Empfangsstationen zur Verfügung. Bei geostationären Erdfernerkundungssatelliten ist die Position des Satelliten zur Erde konstant, so dass eine kontinuierliche Kommunikation zwischen dem Satelliten und der Bodenstation möglich ist. Bei allen Satelliten mit erdfernerer oder erdnäherer Umlaufbahn verändert sich die Position des Satelliten fortlaufend und nur während des Überfliegens des Satelliten über die Empfangsstation kann mit dem Satelliten Kontakt aufgenommen werden. Diese Kontaktzeiten ergeben sich aus der Geschwindigkeit des Satelliten und der Entfernung des Satelliten zur Erde und liegt zwischen ca. 7 und 10 Minuten bei Satelliten mit einer Höhe von 600 bis 800 km über der Erdoberfläche – was derzeit der am häufigsten verwendeten Höhe von Erdfernerkundungssatelliten entspricht. Die Daten werden mit Antennen oder Antennenfeldern empfangen. Man spricht hier von einem „Downlink“.

Als Downlink bezeichnet man die Kommunikation vom Satelliten zur Bodenstation. Es gibt zum einen den S-Band Downlink, der aus Telemetrie-Daten besteht und zum anderen den X-Band Downlink, der die Nutzlastdaten (in diesem Fall Radardaten) beinhaltet. Telemetrie-Daten enthalten alle relevanten Daten über den Zustand des Satelliten und seinen Elementen. Die Downlinkinfo-Datei wird vom Missionsbetriebssegment (MOS) zur Verfügung gestellt und enthält alle Informationen, die die Bodenstation benötigt, um Daten von dem Satelliten zu empfangen.

Zur heutigen Zeit, wo die zu transferierenden Datenmengen zur Erde stetig wachsen, existiert ein weltweites Netz an Bodenstationen. Teilweise werden auch Bodenstationen aufgebaut, die nur temporär in sogenannten Kampagnen Verwendung finden. Jede Empfangsstation besitzt einen Sichtbarkeitskreis. Dies ist der Bereich in dem die Bodenstation Funkkontakt zum Satelliten haben kann [siehe Abbildung 4].

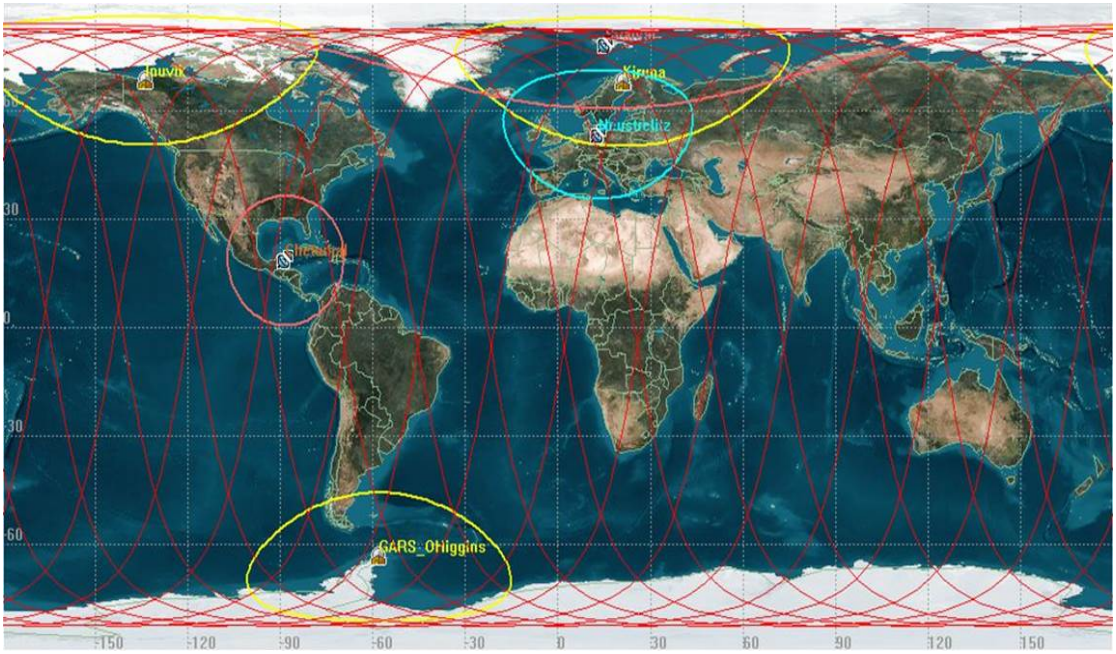

Abbildung 2-1 Sichtbarkeitskreise der Empfangsstationen des DLR [DLR02]

Nutzlastbodensegment

Als Nutzlast werden die Elemente bezeichnet, die von einem Raumfahrzeug transportiert werden, um (zumeist wissenschaftliche) Daten zu erheben, also das eigentliche Instrument oder der Sensor. Die aufgenommenen Daten bezeichnet man als Nutzlastdaten. Das Nutzlastbodensegment besteht aus untereinander vernetzten Sende-

und Empfangsstationen sowie Betriebseinrichtungen zur weiteren Verarbeitung und Speicherung der Nutzlastdaten.

Missionsbetriebssegment

Dem Missionsbetrieb unterliegt eine zentrale Aufgabe bei der Vorbereitung und Durchführung von Satellitenmissionen. Bei der Missionsplanung werden im Vorfeld sämtliche Informationen, Ressourcen und Anforderungen gesammelt und analysiert. Während der Mission müssen die Aktivitäten des Satelliten und die Aktivitäten am Boden effizient geplant und dokumentiert werden. Um den Zeitaufwand und die Risiken bei dem Aufbau des Bodensystems für neue Missionen zu vermindern, soll auf getestete und praxisbewährte Bausteine zurückgegriffen werden. Hauptaufgaben des Missionsbetriebssegments sind die Kommandierung und die Kontrolle der Satelliten. Außerdem führt es Analysen über die Umlaufbahn durch, plant die Aufnahmen und stellt Zusatzdaten für die Verarbeitung der Nutzlastdaten bereit. Der Missionsbetrieb ist auch für die Erstellung und Verwaltung der von der Ver- und Entschlüsselung benötigten kryptographischen Schlüssel zuständig. Diese Komponente nennt sich Key Management Facility (KMF). Sie ist zum einen für die Verschlüsselung der Satellitenkommandos vor dem „Uplink“, also dem Senden von Daten zum Satelliten und für die Verschlüsselungen der Nutzlastdaten auf dem Satelliten vor dem „Downlink“ verantwortlich, sowie für die Zurverfügungstellung der Schlüssel für die Entschlüsselung am Boden.

Instrumentenbetriebs- und Kalibrierungseinrichtung

Die Instrumentenbetriebs- und Kalibrierungseinrichtung ist für den Betrieb der Instrumente zuständig, überwacht also die Instrumente und die Kalibrierung des Systems.

2.2 Das Satellitendatensicherheitsgesetz (SatDSiG)

Das SatDSiG ist ein Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten [BJV07]. Hochwertige Erdfernerkundungsdaten bezeichnen Daten mit besonders hohem Informationsgehalt. Dieser hohe Informationsgehalt ergibt sich aus der geometrischen, zeitlichen, radiometrischen und spektralen Auflösung, der spektralen Abdeckung und der Anzahl der Spektralkanäle. Bei Radar- oder

Mikrowellensensoren fließen noch Phasenlage und Polarisationsmerkmale in die Betrachtung mit ein. [BMW08]

Zweck

Dieses Gesetz wurde hauptsächlich aus zwei Gründen verabschiedet. Der erste bestand in der Wahrung der sicherheits- und außenpolitischen Interessen der Bundesrepublik Deutschland bei der kommerziellen Vermarktung und Verbreitung von hochwertigen Erdfernerkundungsdaten. Der zweite Grund war, dass dadurch eine wichtige Voraussetzung geschaffen wurde, damit deutsche Unternehmen Satellitenanwendungen in wirtschaftlich tragfähige Geschäftsmodelle umsetzen und neue Absatzmärkte erschließen können. [BMW08]

Anlass

Durch den beachtlichen Fortschritt bei der Entwicklung von Erdfernerkundungssensoren werden Daten und Datenprodukte mit hoher Qualität erzeugt. Diese qualitativ hochwertigen Daten wurden vorher nur im militärischen Bereich genutzt, jedoch soll die Verbreitung der Erdfernerkundungsdaten auch durch kommerzielle Anbieter ermöglicht werden. Ein Großteil der Daten kann ohne Risiko verbreitet werden. Jedoch verursachen Kombinationen von mehreren Kriterien bei den Erdfernerkundungsdaten, sowohl bei der Übertragung als auch bei der Verbreitung, Gefährdungen der Sicherheit der Bundesrepublik Deutschland. Da im deutschen Recht keine diesbezügliche Regelung existierte, wurde eine gesetzliche Grundlage notwendig, welche die Verbreitung der Erdfernerkundungsdaten derartiger Qualität durch kommerzielle Anbieter regelt. [BRD07]

Regelungsgegenstand und -aspekte

Das Gesetz regelt die Datenübertragung auf dem Boden und zwischen Satelliten und Bodenstationen. Jedes hochwertige Erdfernerkundungssystem, welches Daten verbreiten möchte, benötigt eine Zulassung. Diese Zulassung ist über das Gesetz geregelt. Die Daten dürfen nur an Personen ausgeliefert werden, die nicht in einer EU-Sanktionsliste stehen. Für jede Datenanfrage von einem Kunden muss durch den Anbieter der Daten eine Sensitivitätsprüfung durchgeführt werden. Bei der Sensitivitätsprüfung werden Parameter zugrunde gelegt, die aus der aktuellen Verordnung zum SatDSiG (Satellitendatensicherheitsverordnung – SatDSiV) [BJV08]

entnommen werden. Alle Personen, die Zugang zu Kommandierungsanlagen oder den Anlagen zum Empfang, zur Verarbeitung oder zur Speicherung von Daten haben, sind einer einfachen Sicherheitsüberprüfung (Ü1) zu unterziehen. Im Rahmen des Auftragsabwicklungsprozesses gemäß §5 (1) und (2) und §18 (1) und (2) des SatDSiG [BJV07] müssen bestimmte Daten aufgezeichnet und mindestens fünf Jahre lang aufbewahrt werden.

2.3 Informationssicherheit

In der Literatur findet sich keine allgemeine Definition des Begriffes Sicherheit, der in der Informationstechnik durch die beiden englischen Begriffe Security und Safety geprägt ist [Fr14]. Deshalb sollen zunächst die englischen Begriffe Security und Safety unterschieden werden.
Eckert übersetzt **Safety** mit Funktionssicherheit. Ein funktionssicheres System nimmt keine funktional unzulässigen Zustände ein. **Security** wird von Eckert mit Informationssicherheit übersetzt. Safety heißt folglich, das System funktioniert unter normalen Betriebsbedingungen wie vorgesehen. Bei Security wird die Widerstandsfähigkeit von IT-Systemen gegenüber Angreifern betrachtet. [Ec14, S. 6f].

In dieser Arbeit werden die Begriffe von Eckert verwendet und es wird immer im Sinne von Security und nicht Safety gesprochen, wenn von Sicherheit die Rede ist.
Die beiden Begriffe Informationssicherheit und IT-Sicherheit werden häufig im deutschen Sprachgebrauch synonym verwendet. IT steht für die Abkürzungen "Informationstechnik", "Informations- und Kommunikationstechnik" oder "Informations- und Telekommunikationstechnik".
Der Begriff Informationssicherheit ist im Gegensatz zu IT-Sicherheit umfassender. Im weiteren Verlauf der Arbeit wird der Begriff Informationssicherheit verwendet. Die Informationssicherheit, wie auch die IT-Sicherheit, folgt der technischen Entwicklung und muss an ständige Veränderungen dynamisch angepasst werden.
„Informationssicherheit hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft. Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung“ [BSI01].

Zum Erreichen bzw. Einhalten der Informationssicherheit werden Schutzziele definiert. Die Informationssicherheit ist bestrebt bestehende Bedrohungen für die Schutzziele durch angemessene Maßnahmen auf ein tragbares Maß zu reduzieren. [Ec14]. Die Schutzziele werden im nächsten Unterkapitel näher beschrieben.
Daten und Informationen werden in dieser Arbeit gleichbedeutend verwendet. Die Informationen werden durch Daten bzw. Datenobjekte repräsentiert [Ec14, S. 4f].
Wo möglich werden deutsche Begriffe verwendet. Um die Begriffe zu verwenden, die in der Informationssicherheit gebräuchlich sind, wird in dieser Arbeit bei einigen Definitionen der Risikoanalyse der englische Begriff verwendet.

2.3.1 Schutzziele

An dieser Stelle sollen die Schutzziele der Informationssicherheit diskutiert werden - anhand dieser wird häufig die Informationssicherheit definiert. Damit die Definitionen besser vergleichbar sind, werden zusätzlich die entsprechenden englischen Begriffe genannt. Die Definitionen der Begriffe sind an die Ausführungen in Bender und Ackermann [BA10], Eckert [Ec14], Dierstein [Di04], ISO 27000-Normen [ISO14] und Anderson [An08] angelehnt.

Im Folgenden werden nur die für die Arbeit relevanten Schutzziele vorgestellt. Es werden zugleich die englischen Begriffsdefinitionen aus dem ISO-Standard ISO/IEC 27000 bereitgestellt. Einige vorgestellte Schutzziele besitzen keine äquivalente Begriffsdefinition bei dem ISO-Standard für Informationssicherheit:

Vertraulichkeit (confidentiality):

Die zu schützenden Informationen dürfen nur für befugte Nutzer zugänglich sein.

ISO/IEC 27000: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Hierfür muss klar festgelegt werden, welche Personen, welcher Prozess und welches System, im Weiteren als Subjekt bezeichnet, für den Zugriff auf die Daten berechtigt wird. Eine Verletzung der Vertraulichkeit liegt dann vor, wenn ein unberechtigtes Subjekt die zu schützenden Informationen einsehen kann.

Integrität (integrity):

Die Informationen sind vor unerlaubten und unbemerkten Veränderungen geschützt.

ISO/IEC 27000: property of protecting the accuracy and completeness of assets

Dieses Schutzziel wird technisch durch Zugriffrechte realisiert. In Umgebungen, wie zum Beispiel dem Internet, in der eine Datenmanipulation kaum verhindert werden kann, werden zur Erkennung von Änderungen an den Daten kryptografisch sichere Hashfunktionen verwendet [Ec14, S. 9].

Verfügbarkeit (availability):

Die gewünschte Nutzung der Daten ist autorisierten und authentifizierten Subjekten bei Bedarf möglich.

ISO/IEC 27000: property of being accessible and usable upon demand by an authorized entity

Bei diesem Schutzziel muss sichergestellt werden, dass die Anfrage in entsprechender Zeit beantwortet wird. Durch temporäre hohe Beanspruchung des Systems kann es zu zeitlichen Verzögerungen kommen, die, sofern sie „normal“ sind, als autorisierte Beeinträchtigungen betrachtet werden. Die Schwierigkeit liegt nun darin, festzustellen, ob eine autorisierte Beeinträchtigung oder eine unautorisierte Beeinträchtigung, die ggf. durch einen Angriff hervorgerufen wurde, vorliegt [Ec14, S. 12].

Für Anwendungen werden diese drei Hauptziele noch durch folgende Ziele ergänzt:

Authentizität (authenticity):

Die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts kann anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüft werden.

ISO/IEC 27000: property that an entity is what it is claims to be

Um dieses Schutzziel zu gewährleisten, muss durch geeignete Kontrollmaßnahmen sichergestellt werden, dass das Objekt bzw. Subjekt das ist, was es vorgibt zu sein. Bei diesen Kontrollmaßnahmen können sich beispielweise Personen über die Kenntnis eines Passwortes, durch den Besitz einer Chipkarte bzw. eines digitalen Zertifikats oder durch biometrische Merkmale (Fingerabdruck, Irismerkmale) gegenüber einem System authentisieren [Ec14, S. 8f].

Zu unterscheiden ist zwischen Authentizität und Autorisierung.

Autorisierung (authorization):

> Ein Subjekt besitzt die Berechtigung, auf eine Information bzw. sein Datenobjekt zuzugreifen, das Subjekt ist zu diesem Zugriff autorisiert. [Ec14, S. 5]

Dieses Schutzziel wird über Zugriffsrechte geregelt. Im Vergleich zur Authentisierung die eine behauptete Identität verifiziert, wird bei der Autorisierung überprüft, ob das zuvor authentisierte Subjekt befugt ist, bestimmte Aktionen auszuführen [BSI04], [BSI05]. Die Autorisierung, d. h. die Zuweisung von Rechten erfolgt nach der erfolgreichen Authentisierung.

Verbindlichkeit oder Zuordenbarkeit (non repudiation):

> Aktionen, die ein Subjekt ausgeführt hat, können im Nachhinein nicht abgestritten werden.

ISO/IEC 27000: ability to prove the occurrence of a claimed event or action and its originating entities

Dieses Schutzziel erlangt vor allem in dem Bereich des elektronischen Handels und der elektronischen Geschäfte große Bedeutung. Aber auch beispielsweise bei Peer-to-Peer-Computing ist dieses Schutzziel für den Nachweis der Abrechenbarkeit (siehe nächstes Schutzziel) notwendig [Ec14, S. 12f].

Zurechenbarkeit oder Abrechenbarkeit (accountability):

> „Von jeder in einem IT-System ausgeführten Aktion (Vorgang, Prozess) muss während ihres Ablaufs und danach feststellbar sein, wem, d.h. welcher Instanz – insbesondere welcher Person – diese Aktion zuzuordnen ist, welches Subjekt sie ausgelöst und wer sie letztlich zu verantworten hat“ [Di04].

ISO/IEC 27000: responsibility of an entity for its actions and decisions

Dieses Schutzziel „erfordert Maßnahmen zur Überwachung (engl. audit) sowie zur Protokollierung einzelner Benutzeraktivitäten“ [Ec14, S. 13].

Revisionsfähigkeit (*reviewability*):

> Revisionsfähigkeit bedeutet Nachprüfbarkeit und Nachvollziehbarkeit. Hiermit soll lückenlos festgestellt werden wer, wann, welche Daten wie verarbeitet hat [BA10].

Dies bedeutet, dass bereits bei der Planung des Systems Vorkehrungen getroffen werden müssen, damit die korrekte Verarbeitung der Daten kontrolliert werden kann.

2.4 Security Engineering

Bisher hat in der Praxis eine systematische Entwicklung von Security Engineering kaum stattgefunden. Die Gründe hierfür sind vielfältig. Zum einen, ist Sicherheit keine funktionale Anforderung und kann schwer erfasst und bewertet werden, zum anderen stehen die heutigen Systementwicklungen unter Termindruck, so dass die Sicherheitsmaßnahmen oft vernachlässigt werden. Hinzu kommt, dass die Entwickler von komplexen Systemen häufig keine Sicherheitsexperten sind.

Die Disziplin Security Engineering ist grundlegend von Ross Anderson geprägt. Diese Disziplin konzentriert sich auf die Werkzeuge, Prozesse und Methoden für das Design, die Implementierung und das Testen von abgeschlossenen Systemen, bestehenden Systemen und Systemen die sich an ihre ändernden Umweltbedingungen anpassen, und die notwendig sind, um auch bei Angriffen oder bei fehlerhaften Umgang deren Zuverlässigkeit sicherzustellen [An08, S. 3]. Laut Anderson ist Security Engineering disziplinübergreifend und erfordert Fachkenntnisse in juristischen, wirtschaftlichen sowie psychologischen Aspekten.

Die Bemühungen für die Herstellung von sicheren Systemen haben sich dabei laut Eckert überwiegend auf Werkzeuge und Methoden zur Herstellung von modell-getriebenen sicheren Systemen beschränkt [Ec14, S. 184f].

2.5 Risikoanalyse

Die Risikoanalyse ist ein weit verbreitetes und in vielen Gebieten eingesetztes Verfahren, um Gefahrenszenarien zu beurteilen. Hierbei wird versucht, vorhandene Risiken zu erkennen, zu bewerten und zu behandeln, um negative Folgen weitestgehend zu reduzieren. Eine detaillierte Analyse benötigt sehr viel Zeit und verursacht hohe Kosten. Wichtig ist, dass keine Bedrohung unbeachtet bleibt und alle Schritte sorgfältig dokumentiert sind, damit sie nachvollziehbar sind. Das Ziel der Risikoanalyse ist die Bereitstellung von Informationen, die für die Entscheidungsfindung zugunsten von genannten Maßnahmen in Unternehmen unerlässlich sind. [Sp09], [RSH91], [Ci97], [Ro08], [NIS14]

Im Bereich der Informationssicherheit gibt es eine Vielzahl von Risikoanalysemethoden. Diese unterschiedlichen Methoden kann man in zwei Hauptkategorien einteilen, zum einen in die qualitative Risikoanalyse, zum anderen in die quantitative Risikoanalyse. Obwohl eine große Anzahl dieser verschiedenen Methoden existieren, ist es schwierig, eine Methode zu finden, die alle Anforderungen einer Organisation erfüllt. [RSH91], [Ci97], [Li96]

Bei der quantitativen Risikoanalyse wird versucht, den Wahrscheinlichkeiten, dass bestimmte Risiken auftreten sowie ihrem Schadensausmaß, Zahlenwerte zuzuordnen. Die Zahlenwerte beruhen auf den mathematischen Modellen der Statistik und der Wahrscheinlichkeitsrechnung unter Verwendung von historischen Daten.
Mit Hilfe dieser Zahlenwerte kann man die Kosten zwischen der Schadensvermeidung und den vorgeschlagenen Gegenmaßnahmen genau berechnen. Meistens ist es jedoch sehr schwierig die genaue Wahrscheinlichkeit und den Schaden jedes einzelnen Risikos genau zu bestimmen. Deswegen wird häufig die qualitative Risikoanalyse verwendet. Bei einer qualitativen Risikoanalyse wird ein Risiko, ebenso wie bei der quantitativen Risikoanalyse, nach seiner Eintrittswahrscheinlichkeit und seinen Auswirkungen eingeschätzt und priorisiert. Jedoch werden hier die Einschätzungen nicht genau beziffert, sondern mit beschreibenden Werten, wie „hoch“, „mittel“ oder „sehr niedrig“ bewertet. Hierbei werden die Risiken durch Erfahrungswerte, persönliches Urteil oder Vergleiche betrachtet. Die qualitative Risikoanalyse geht oft der quantitativen Risikoanalyse voraus, die sich dann im Allgemeinen auf die Risiken mit hoher Priorität konzentriert. Die qualitative Risikoanalyse ist kostengünstiger und einfacher durchzuführen, da sie nicht so viel Erfahrung und Aufwand für ihre Durchführung benötigt wie die quantitative Risikoanalyse. Jedoch ist die Durchführung einer Kosten-Nutzen-Analyse für die Entscheidung, welche Gegenmaßnahmen für die Vermeidung bzw. Verminderung des zu erwartenden Schadensausmaßes verwendet werden sollen, weitaus schwieriger als bei der quantitativen Risikoanalyse. [SWH13], [Le14], [RSH91]

In den letzten Jahren verursachten Begriffsdefinitionen im Bereich der Risikoanalyse und der Informationssicherheit intensive Diskussionen in Deutschland, da teilweise synonyme Begriffe mit verschiedenen Bedeutungen benutzt werden [Fr14].

Deswegen werden in dieser Masterarbeit, in Anlehnung an [Ec14], folgende Begriffsdefinitionen bei der Ausübung einer Risikoanalyse in Zusammenhang mit Informationssicherheit verwendet.

Schützenswerte Güter (engl. assets) umfassen Informationen und Objekte, die sie repräsentieren [Ec14, S. 4]. Diese Güter sind wichtig für einen Eigentümer und müssen deswegen geschützt werden. Je wertvoller ein Gut ist, umso mehr muss es geschützt werden. Diese Güter sind unterschiedlichen Bedrohungen ausgesetzt. Dies kann von Hardwareausfällen bis hin zu kriminellen Angriffen reichen.

Eine **Bedrohung** (engl. threat) des Systems zielt darauf ab, dass eine Schwachstelle entdeckt und diese Schwachstelle zur Verursachung eines Schadens ausgenutzt wird. Der Schaden kann durch den Verlust der Datenintegrität, der Informationsvertraulichkeit, der Verfügbarkeit oder der Authentizität erstehen [Ec14, S 17].

„Unter dem **Risiko** (engl. risk) einer Bedrohung verstehen wir die Wahrscheinlichkeit (oder relative Häufigkeit) des Eintritts eines Schadensereignisses und die Höhe des potenziellen Schadens, der dadurch hervorgerufen werden kann“ [Ec14, S. 18].

Der Begriff **Bedrohungsagent** (engl. threat agent) wird bei [Ec14] nicht definiert, sie verwendet den Begriff Angreifertyp [Ec14], S. 205. Der Begriff soll jedoch an dieser Stelle definiert werden, da er bei der Anwendung der Methode Verwendung findet.
Gemäß [CC01, S. 19] bedeutet threat agent: *entity that can adversely act on assets*.
Die Bedrohungsagenten sind demnach Einflüsse, die eine oder mehrere Schwachstellen ausnutzen, um die Schutzziele eines Systems zu gefährden und sich dadurch nachteilig auf ein schützenswertes Gut auswirken. Beispiele hierfür sind Hacker, Viren, Schadsoftware oder bestimmte Personen.

Eine **Schwachstelle** (engl. weakness), ist eine Stelle im System, an dem das System verwundbar werden kann. Sobald ein threat bzw. ein threat agent existiert, der diese Sicherheitslücke ausnützt, wird diese Schwachstelle zu einer **Verwundbarkeit** (vulnerability). Die Verwundbarkeit ist demnach eine Untermenge der Schwachstellen. [Ec14, S. 16]

„Unter einem **Angriff** (engl. attack) verstehen wir einen nicht autorisierten Zugriff bzw. einen nicht autorisierten Zugriffsversuch auf das System. Wir unterscheiden passive und aktive Angriffe. Passive Angriffe betreffen die unautorisierte Informationsgewinnung und zielen auf den Verlust der Vertraulichkeit ab. Aktive Angriffe betreffen die unautorisierte Modifikation von Datenobjekten und richten sich somit gegen die Datenintegrität oder Verfügbarkeit eines Systems“ [Ec14, S. 19].

Gegenmaßnahmen (engl. countermeasures, controls oder auch safeguards genannt) dienen dazu, Risiken zu identifizierten und ihnen entgegen zu wirken.
„Durch geeignete Gegenmaßnahmen können Schwachstellen kompensiert oder zumindest eingegrenzt, in einigen Fällen sogar eliminiert werden, sodass dadurch das von Bedrohungen ausgehende Gefährdungspotenzial reduziert bzw. annulliert werden kann“ [Fr14].

Im weiteren Verlauf der Masterarbeit werden zunächst die Bedrohungen, die mögliche Schäden an einem System verursachen könnten, kategorisiert (siehe 2.5.1). Danach werden die Risiken bewertet (2.5.2) und anschließend die unterschiedlichen Arten aufgeführt, wie Risiken behandelt werden können (2.5.3).

2.5.1 Bedrohungskategorien

Die eigentlichen Ursachen möglicher Schäden werden durch Bedrohungsklassen beschrieben. Auf die Anwendung gerichtete Angriffe können aufgrund deren Zweck und Ziel eingeordnet werden.
Innerhalb der TVRA werden folgende vier Kategorien [ETS11, S. 25f] verwendet, die an dieser Stelle näher beschrieben werden:

- Abfangen (engl. interception):
  - Lauschen (engl. eavesdropping): Abhören von Daten.
- Manipulation (engl. manipulation oder auch tampering genannt): Diese Kategorie besitzt noch folgende Unterkategorien:
  - Vortäuschen (engl. spoofing): Vorgeben jemand anderes zu sein und mittels dieser falschen Identität Zugriff auf ein System zu erlangen.

    - Verlust oder Verfälschen von Daten (engl. loss oder corruption): Unbefugtes Löschen, Einfügen, Ändern, Nachbestellen bzw. erneutes oder verzögertes Übertragen von Daten.
    - Unautorisierter Zugriff (engl. unauthorized access): Zugriff auf Daten ohne Berechtigung auf Daten.
    - Fälschung (engl. forgery): Verschicken der Daten mit der Behauptung, dass diese Informationen von einer anderen Partei empfangen oder an eine andere Einheit gesendet wurde.
- Ablehnung (engl. repudiation): Möglichkeit, die von einem Benutzer durchgeführten Aktionen zu leugnen. Bei Kommunikationsnetzen bedeutet dies, die Verleugnung der Teilnahme an einer Kommunikation durch den Sender oder den Empfänger.
- Dienstverweigerung/Dienstverhinderung (denial of service): Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte. Die Ressourcen eines Systems werden verbraucht, so dass es zu einer Überlastung eines Systems kommt und das System für seine eigentlichen Aufgaben nicht mehr zur Verfügung steht. Bei Kommunikationsnetzten bedeutet dies die Verhinderung/Unterbrechung der Kommunikationsbeziehung.

Zusätzlich sollen noch zwei weitere Kategorien beschrieben werden, die in dem weiteren Verlauf der Arbeit verwendet werden.

- Offenlegung von Informationen (engl. information disclosure): Unerwünschte Offenlegung privater Daten.
- Erweiterung der Berechtigung (engl. elevation of privilege): Jemandem erlauben etwas zu tun, zu dem er keine Berechtigung hat.

Die näheren Ausführungen zu den Kategorien stammen aus [Ms01] und [Sh14].

Anhand dieser Kategorien können die gefundenen Risiken eingeordnet, ihr Schutzbedarf festgestellt und ggf. ihre Gegenmaßnahmen ermittelt werden.

2.5.2 Risiken bewerten

Sobald alle Risiken identifiziert und analysiert worden sind, erfolgt anschließend eine Bewertung der Risiken. Risiken sollten priorisiert werden, damit die wichtigsten zuerst behandelt werden und nicht die, die am einfachsten behoben werden können. Um ein Risiko zu bewerten und damit eine mögliche Verletzung eines Schutzziels greifbarer zu machen, benötigt man die Variablen Eintrittswahrscheinlichkeit und Schadenshöhe bei Eintritt des Schadens. Der quantitative Wert des Risikos berechnet sich dann wie folgt:

Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe bei Eintritt

[Ec14, S. 204]

Beim einfachen Verfahren der Risikobewertung werden diese Variablen abgeschätzt und die Risiken mit einem hohen Risikowert werden priorisiert.

2.5.3 Risiken behandeln

Grundsätzlich gibt es vier Ansätze zur Behandlung von Risiken, die in [Kö13, S. 61] beschrieben sind:

Risiko vermeiden, durch entsprechende Maßnahmen, was leider nicht immer möglich ist.

Risiko akzeptieren, da ein Risiko zugleich auch immer eine Chance bedeutet. So kann es möglicherweise besser sein, das Risiko zu akzeptieren und mögliche Chancen zu nutzen, als es durch hohen Kostenaufwand zu vermeiden.

Risiko transferieren, um das Risiko aus dem eigenen Verantwortungsbereich zu verlagern. Dies kann durch Vereinbarungen mit anderen Beteiligten, z.B.: Versicherungen oder Lieferanten, geschehen, so dass diese die Verantwortung des Risikos übernehmen.

Risiko steuern, indem durch entsprechende Maßnahmen die Eintrittswahrscheinlichkeit oder der mögliche Schaden im Falle des Eintritts reduziert wird.

2.6 Common Criteria/Common Methodology

Die Verwendung von etablierten Standards bei der Risikoanalyse hilft, die IT-Risiken umfassend zu ermitteln und die Schutzmechanismen nicht aufwendiger zu gestalten, als es das Risiko verlangt. Mit den CC, die auch unter der Bezeichnung ISO/IEC 15408

bekannt sind, wurden Kriterien für einen internationalen Standard entwickelt, die weltweit anerkannt und gültig sind.

Der Kriterienkatalog dient zur Prüfung und Bewertung von Sicherheit in der Informationstechnologie und hilft, Vertrauen in die Wirksamkeit von evaluierten IT-Systemen zu schaffen [Ec14, S. 236f].

Die CC umfasst drei Teile:
Teil 1: Einführung und allgemeines Modell (Introduction and General Model) [CC01]
In diesem Teil wird ein Überblick über die erforderlichen Dokumente gegeben, die für die Evaluierung des Evaluierungsgegenstandes benötigt werden.
Teil 2: Funktionale Sicherheitsanforderungen (Security Functional Requirements,SFR) [CC02]
Dieser Teil beschreibt die Kriterien und Anforderungen an Sicherheitsfunktionen.
Teil 3: Anforderungen an die Vertrauenswürdigkeit (Assurance Requirements) [CC03]
Die Beschreibung der Kriterien zur Evaluierung von Schutzprofilen und der Sicherheitsvorgaben für die Vertrauenswürdigkeit sind in diesem Teil vorhanden.

Im Sinne der CC sollen schützenswerte Informationen vor dem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität bewahrt werden. Es werden hierbei nicht nur funktionale Anforderungen und Anforderungen an die Vertrauenswürdigkeit berücksichtigt, sondern auch die unmittelbare Umgebung betrachtet.

Ergänzend zu den CC wurde eine Zertifizierungsmethodik entwickelt, die die Vorgehensweise für die Prüfung definiert. Diese Common Evaluation Methodology [CEM] stellt sicher, dass die Ergebnisse von Zertifizierungen nachvollziehbar und vergleichbar sind [VH07].

Gemäß den CC ist ein **Evaluations- oder Evaluierungsgegenstand (target of evaluation (TOE))** ein IT-Produkt, eine IT-Komponente oder ein IT-System und die zugehörige Begleitdokumentation, das bzw. die auf Erfüllung aller Sicherheitsanforderungen zu evaluieren ist. Nähere Erläuterungen können unter [CC01, S. 32]) nachgelesen werden. Die Verwendung eines Evaluationsgegenstandes soll dazu führen, dass die Ergebnisse der Analyse objektiv und wiederholbar sind [Kr03, S. 231]).

Die Menge der Sicherheitsanforderungen, die bei der Evaluation für ein bestimmtes TOE verwendet wird, wird im CC als **Security Target (ST)** bezeichnet. Die Security Targets sind implementierungsabhängig [CC01, S. 19]. Sie sind die Sicherheitsvorgaben und der Ausgangspunkt eines Produkts.

Schutzprofile (protection profiles (PPs)) sind implementierungsunabhängige Anforderungen an die Funktionalität und die Vertrauenswürdigkeit bestimmter Produktgruppen. Sie werden für Standardsicherheitsprobleme verwendet und beschreiben ein Konzept. Diese Schutzprofile sind vollständig und konsistent und dienen als Nachweis für Evaluierungsverfahren. Die erfolgreiche Evaluierung wird durch ein Zertifikat bestätigt. [CC01, S. 50ff.]

3 Methoden zur Analyse von IT-Sicherheitsrisiken

IT Risikomanagement spielt zur heutigen Zeit in vielen Unternehmen eine immer wichtigere Rolle und ist eine sehr komplexe Angelegenheit. Einer ihrer wichtigsten Prozesse ist die Risikoanalyse. In den letzten Jahren sind viele verschiedene nationale und internationale Rahmenwerke für das IT-Risikomanagement und der Risikoanalyse veröffentlicht worden, wie zum Beispiel ISO/IEC 27005 [ISO14] oder NIST [NIS14]. Diese Standards stellen Definitionen, Anforderungen und Richtlinien für die Implementierung und Verwaltung von Informationssicherheitssystemen zur Verfügung. Sie werden konstant auf dem neuesten Stand gehalten und bieten so eine gute Orientierung, um sensitive Informationen zu sichern und zu schützen. An dieser Stelle der Arbeit sollen einige untersuchte Risikoanalysemethoden vorgestellt werden. Der Überblick ist nicht vollständig, sondern es wurden einige Methoden aufgrund ihrer Relevanz innerhalb der Informationssicherheit ausgewählt.

3.1 Untersuchung verschiedener Analysemethoden für die Identifizierung von Risiken der Informationssicherheit

Es gibt eine Vielzahl an Methoden zur Analyse von IT-Sicherheitsrisiken. Sie lassen sich unterteilen in quantitative und in qualitative Methoden. Beide Herangehensweisen haben Vor- und Nachteile: In seinem Artikel „*IT Risk Assessment: Quantitative and Qualitative Approach*“ [Ro08] fasst Artur Rot diese Vor- und Nachteile wie in der nachfolgenden Tabelle zusammen:

	Quantitativ	**Qualitativ**
Vorteile	• Sie ermöglichen eine quantitative Darstellung des Schadensausmaßes, dadurch wird die Kosten-Nutzen-Analyse für die Auswahl von Schutzmaßnahmen erleichtert. • Sie geben ein genaueres Bild der Risiken.	• Die Methoden ermöglichen die Risiken nach Prioritäten zu ordnen. • Sie ermöglicht die Bestimmung der Risiken mit der größten Gefahr in einer kurzen Zeit und ohne größeren Aufwand. • Die Analyse ist relativ einfach und billig.
Nachteile	• Quantitative Messungen sind abhängig von Umfang und Genauigkeit definierter Messskalen. • Die Ergebnisse der Analyse	• Die Bestimmung von Wahrscheinlichkeiten und quantitativen Ergebnissen wird nicht unterstützt. • Die Kosten-Nutzen-Analyse für

	können unpräzise und sogar verwirrend sein. • Normale Methoden müssen mit qualitativen Beschreibungen angereichert werden (In Form von Kommentaren, Interpretationen). • Die Anwendung dieser Methoden ist in der Regel teurer und fordert mehr Erfahrung und erweiterte Tools.	die Auswahl von Schutzmaßnahmen ist schwieriger. • Die Ergebnisse haben allgemeinen Charakter.

Tabelle 3-1 Vor- und Nachteile von quantitativen und qualitativen Analysemethoden [Ro08]

Im Folgenden werden drei quantitative (MAGERIT, ISRAM, IS) und drei qualitative (OCTAVE, CRAMM, TVRA) Risikoanalysemethoden vorgestellt.

Quantitative Methoden:

MAGERIT (Metodología de Análisis y GEstión de RIesgos del MinisTerio de Administraciones Públicas):

MAGERIT wurde vom spanischen Ministerium für Behörden der öffentlichen Verwaltungen entwickelt, kann aber auch für andere Organisationen verwendet werden. Die erste Version wurde 1997 veröffentlicht [Ma14]. MAGERIT besteht aus folgenden fünf Schritten [Ma14, S. 19]:

(1) Bestimmung der schützenswerten Güter für die Organisation, deren Beziehungen untereinander und deren Wert und bezieht sich auf die Kosten, die durch ihre Schädigung verursacht werden.
(2) Bestimmung der Bedrohungen, denen diese schützenswerten Güter ausgesetzt sind.
(3) Bestimmung der zur Verfügung stehenden Schutzmaßnahmen und wie effektiv sie gegen die Bedrohungen wirken.
(4) Schätzen des Schadensausmaßes, im Falle des Eintretens eines Angriffes.
(5) Schätzen des Risikos, welches als das Schadensausmaß definiert wird, gewichtet durch die Häufigkeit des Auftretens (oder der Erwartung des Auftretens) der Bedrohung.

Wie [SHS09] ausführt, umfassen diese Schritte die ersten drei allgemeinen Schritte einer Risikoanalyse: Identifikation der Bedrohung, Identifikation der Verletzlichkeiten und die Risikoermittlung. MAGERIT enthält aber keine Empfehlungen für die Schutzmaßnahmen, dies wird erst im nächsten Schritt des Sicherheitsmanagement nach der Risikoanalyse durchgeführt. MAGERIT ist frei erhältlich [Ki13, S. 3688].

Bei dieser Risikoanalysemethode sind die Gegenmaßnahmen mit den Bedrohungen verbunden und nicht mit den schützenswerten Gütern. MAGERIT ist konform zu ISO 15408 [To02], also den Common Criteria.

ISRAM (Information Security Risk Analysis Method):

Diese Risikoanalysemethode wird ausführlich von Bilge Karabacak und Ibrahim Sogukpinar [KS05] erläutert. Die Information Security Risk Analysis Methode (ISRAM) wurde 2003 im National Research Institute of Electronics and Cryptology und dem Gebze Institute of Technology entwickelt [KS05]. In den Artikeln von [VL05], [SK12] und [BRC12] wird die Methode wie folgt zusammengefasst:

ISRAM ist ein auf Umfragen basierendes Modell, um Risiken in der Informationssicherheit zu analysieren. Hierfür werden für die zwei Eigenschaften eines Risikos - der Eintrittswahrscheinlichkeit und dem Schadensausmaß - unabhängig voneinander zwei separate Umfragen getätigt. Bei ISRAM hat der Risikofaktor einen Wert zwischen 1 und 25. Dieser Wert korrespondiert zu den qualitativen Werten „hoch“, „mittel“ und „niedrig“, wie sie bei Entscheidungen des qualitativen Risikomanagements verwendet werden. Die Methode wird in sieben Schritten durchgeführt. In den ersten vier Schritten wird die Umfrage vorbereitet, im fünften Schritt wird die Umfrage ausgeführt und in den Schritten sechs und sieben werden die Risikowerte ermittelt und die Ergebnisse bewertet.

[KS05] führt als Vorteil dieser Methode im Vergleich zu anderen Methoden an, dass sie einfach anzuwenden ist und keine komplexen mathematischen und statistischen Werkzeuge benötigt werden. Dadurch können Manager und Mitarbeiter einfach in die Analyse einbezogen werden. ISRAM liefert objektive Risikowerte.

[SK12] und [BRC12] führen jedoch an, dass wenn eine Organisation an Einfachheit interessiert ist, ISRAM nicht die richtige Wahl sei. Dennoch wertet sie die Sicherheitsrisiken richtig aus. Die Methode ist frei erhältlich und stimmt mit den Standards NIST SP 800-30, ISO/IEC17799 und ISO/IEC 13335 überein [SK12, S. 32].

IS (IS Risk Analyzed Based of Business Model):

IS Risk Analyzed Based of Business Model wurde 2002 in Süd-Korea am Korea Advanced Institute of Science and Technology (KAIST) entwickelt, da traditionelle Risikoanalysemethoden Einschränkungen hatten [SH03]. Die Methode misst den Wert eines schützenswertes Gutes nicht nur an seinen Wiederbeschaffungskosten, sondern

auch an dem Vermögenswert für den laufenden Betrieb. Das Model besteht aus vier Stufen. Durch dieses Verfahren kann die Bedeutung der verschiedenen Geschäfts-funktionen von dem Geschäftsmodell und die Notwendigkeit von verschiedenen schützenswerten Gütern der Informationssicherheit bestimmt werden. Für die einzelnen Bedrohungen in der Organisation wird mittels mathematischen Formeln die jährliche Verlusterwartung (ALE) berechnet. Das Ergebnis ist ein quantitativer Wert. [VL05], [SK12], [BRC12]

Bei dieser Methode werden extensive mathematische Berechnungen verwendet, dadurch wird die Durchführung sehr zeitaufwendig und kostenintensiv. Als Ergebnis werden objektive und monetäre Werte erhalten, die für die Kosten-Nutzen-Analyse herangezogen werden können. Jedoch betrachtet die Methode keine Abhängigkeiten unter den schützenswerten Gütern. [SH03]

Die Methode ist kostenlos und frei verfügbar, jedoch für Standards nicht anwendbar [SK12, S. 32].

Qualitative Methoden:

OCTAVE (Operational, Critical Threat Analysis and Vulnerability Evaluation):

OCTAVE wurde vom Software Engineering Institute (SEI) der Carnegie Mellon University entwickelt und adressiert sowohl organisatorische als auch technische Risiken [AD03]. Die Methode ist anwendbar für große Unternehmen, für kleinere Organisationen existiert die Variante OCTAVE-S [Ra13].

Bei der Vorgehensweise von OCTAVE stehen die Werte, die Bedrohung und die Schwachstellen im Vordergrund. Für die Durchführung der Risikoanalyse nach OCTAVE wird ein kleines Team benötigt. Dieses Team sollte sich mit den Werten und der Infrastruktur der Organisation auskennen. Das Vorgehen wird in drei Phasen aufgeteilt, wobei jeder dieser Stufen wiederum in Prozesse unterteilt wird. Diese drei Phasen unterteilen sich in:

(1) Aufbauen eines Bedrohungsprofils,
(2) Identifizieren der Schwachstellen der Infrastruktur und
(3) der Entwicklung von Sicherheitsstrategie und Plänen, um die Risiken kritischer Werte zu mildern.

Für den Aufbau des Bedrohungsprofils benutzt OCTAVE eine Erwartungswertmatrix. [AD03],[VL05], [SK12], [BRC12]

Die Werte für die Wahrscheinlichkeit des Eintretens der Bedrohungen und der dadurch verursachte potentielle Schaden sind subjektiv. Diese subjektiven Werte werden dann auf die Erwartungsmatrix angewendet, um dadurch einen Gesamtwert zu erhalten. Es wird nur internes Personal für die Durchführung benötigt und OCTAVE ist relativ einfach zu bedienen. Dadurch sind die Kosten niedrig. Die Analyse basiert auf einzelnen schützenswerten Gütern; es gibt keine Beziehungen zwischen den verschiedenen Risiken. Die Methode ist nicht sehr genau, da keine mathematischen Berechnungen zu Grunde gelegt werden. [Vol05]

Die Methode ist nach einer Anmeldung kostenlos als Probeversion verfügbar [SK12, S. 32]. Für die Durchführung werden Fachwissen und IT-Fähigkeiten benötigt [Ki13]. Die Methode ist für eine Zertifizierung mit Standards jedoch nicht anwendbar.

***CRAMM (CCTA Risk Analysis and Management Method)**:*

Die CCTA Risk Analysis and Management Method wurde 1985 von der Central Computer and Telecommunications Agency (CCTA) der englischen Regierung entwickelt. Sie sollte Behörden der Regierung als Methode für die Überprüfung der Sicherheit von Informationssystemen dienen. Später wurde die Methode an die Britische Firma Insight Consulting verkauft und wird als CRAMM Manager weiter entwickelt.

CRAMM kann für alle Organisationstypen verwendet werden. Für die Erstellung der Datengrundlage behilft sich CRAMM mit Besprechungen, Interviews und strukturierten Fragebögen. Die Methode selbst besteht aus drei Prozessen:

(1) Identifikation und Bewertung der schützenswerten Güter,
(2) Bewertung der Bedrohungen und der Verwundbarkeit, sowie der Berechnung des Risikos,
(3) Auswahl und Empfehlungen der Schutz- und Gegenmaßnahmen.

[Ya02], [BRC12]

Die Methode bietet einen strukturierten Ansatz für eine Risikoanalyse und kann unterstützend verwendet werden für die Zertifizierung nach BS7799 (Britischer Standard, mit der offiziellen Bezeichnung „Code of Practice for Information Security“). Die Methode deckt auch nicht technische Bereiche ab. Die Durchführung der Methode benötigt qualifiziertes und erfahrenes Personal und liefert bei der vollständigen Auswertung sehr viele Ergebnisse, die unter Umständen aufgrund der Verzögerung

zwischen Analyse und Umsetzung nach Änderungen an dem System oder dem Netzwerk bedeutungslos werden könnten. [Ya02]

Die Methode stimmt mit dem internationalen Standard ISO/IEC17799 überein, jedoch werden für die Anwendung der Methode Spezialisten benötigt [SK12, S. 32]. Die Dokumentation ist nicht kostenlos [Ki13, S. 3688].

TVRA (Threat, Vulnerability and Risk Analysis):

Die TVRA wurde von dem ETSI für sogenannte Next Generation Network (NGN) Architekturen entwickelt. Sie ist eine Methode für die Analyse eines Telekommunikationssystems [ETS11]. Die Analyse besteht aus zehn Schritten: Bestimmung des Evaluationsgegenstandes, Identifikation der Schutzziele, Identifikation der funktionalen Sicherheitsanforderungen, systematische Bestandsaufnahme aller schützenswerten Güter, systematische Identifikation der Verwundbarkeiten, Berechnung der Eintrittswahrscheinlichkeit eines Angriffes und seinen Auswirkungen, Aufstellen der Risiken, Identifikation von Sicherheits-Gegenmaßnahmen, Kosten-Nutzen-Analyse der Gegenmaßnahmen, Spezifikation von detaillierten Anforderungen.

In der TVRA werden die Risiken durch das Produkt der Eintrittswahrscheinlichkeiten für die Bedrohungen und den Schadensauswirkungen im Falle, dass ein Schadenereignis auftritt, abgeschätzt. [ETS11]

Laut [ETS11] sind Bedrohungen für ein Telekommunikationssystem stark eingeschränkt und fallen in eine kleine Gruppe von leicht identifizierbaren Kategorien. Unter diese Bedrohungskategorien fallen Abhören, Manipulation, Verleugnung der Teilnahme an einer Kommunikation durch den Sender oder den Empfänger und Denial-of–Service-Angriffen. Die Methode ist somit gut geeignet für den Bereich der Telekommunikationsnetzte, für andere Bereiche dagegen weniger [Es15].

Jede einzelne Methode hat ihre Vor- und Nachteile und sollte für das jeweilige entsprechende Anwendungsgebiet ausgewählt werden. Das Anwendungsgebiet auf das sich diese Masterarbeit fokussiert, ist ein Erdfernerkundungssystem und somit klar in den Bereich der Telekommunikationsnetze einzugliedern. Als eine passende Methode erscheint somit die TVRA-Methode, die zudem noch für eine Zertifizierung nach den allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie

(CC) verwendet werden kann. Dies macht die Ergebnisse der Analyse vergleichbar mit Ergebnissen aus anderen Risikoanalysemethoden.

Die TVRA ist eine qualitative Methode. Dieser Aspekt wurde als positiv für die Auswahl gewertet, da bei einer quantitativen Risikoanalysemethode Daten aus unterschiedlichen Quellen für die Wahrscheinlichkeit und das Ausmaß eines auftretenden Risikos benötigt werden. Diese Daten sind in diesem Fall nicht bekannt. Die TVRA-Methode wurde für die weiteren Ausführungen in dieser Arbeit betrachtet.

Im nächsten Unterkapitel 3.2 wird die Risikoanalyse auf der Basis von IT-Grundschutz näher erläutert. Diese Methode wurde für das bestehende hochwertige Erdfernerkundungssystem in der TanDEM-X Mission angewendet und wird im Unterkapitel 5.3 zum Vergleich herangezogen.

3.2 Risikoanalyse auf der Basis von IT-Grundschutz

Alle Systeme, die der Schutzbedarfskategorie „hoch oder sehr hoch“ zugeordnet sind, müssen neben der Vorgehensweise zur Grundschutzanalyse, gemäß dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), einer detaillierten Risikoanalyse unterzogen werden. Für diese Risikoanalyse können individuelle Sicherheitsmaßnahmen ausgewählt werden. Ein höherwertiges Erdbeobachtungssystem ist in der Schutzbedarfskategorie *sehr hoch* eingestuft und muss demnach einer detaillierten Risikoanalyse unterzogen werden.

Diese Risikoanalyse baut auf einer IT-Strukturanalyse, einer Ermittlung des Schutzbedarfes, einer Modellierung des Systems, einem Basis-Sicherheitscheck und einer ergänzenden Sicherheitsanalyse gemäß der Vorgehensweise des IT-Grundschutzes auf (siehe Abbildung 3-1 Integration der Risikoanalyse in den Sicherheitsprozess [BSI03, S. 5]).

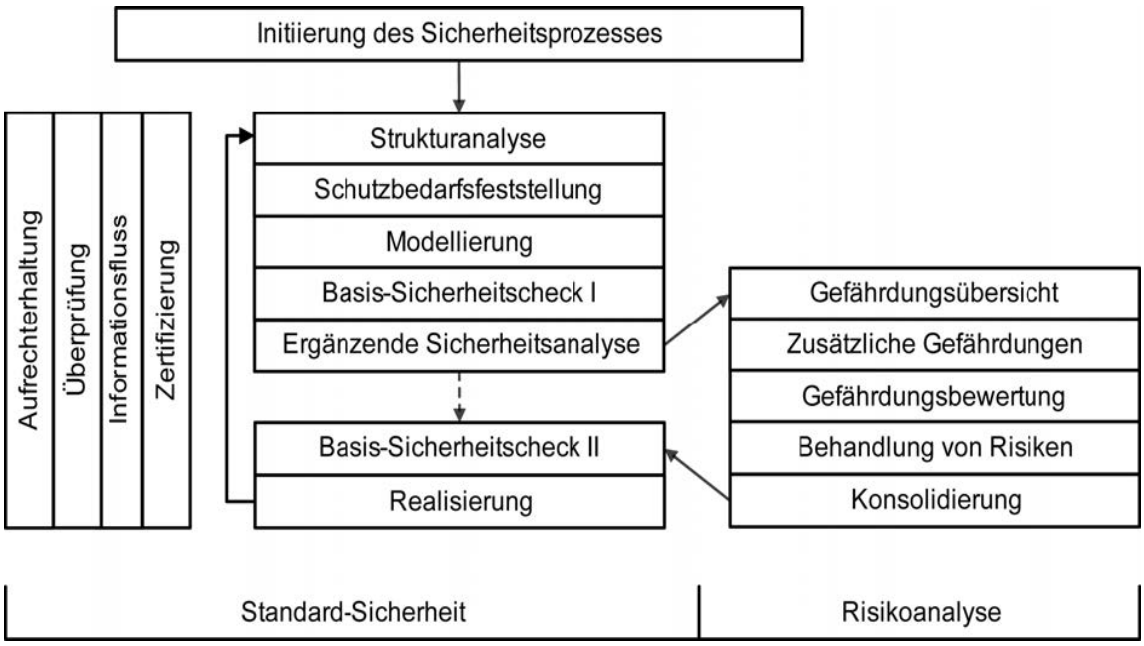

Abbildung 3-1 Integration der Risikoanalyse in den Sicherheitsprozess [BSI03, S. 5]

In der Gefährdungsübersicht werden die schutzbedürftigen Zielobjekte, die für die Risikoanalyse relevant sind, identifiziert und es wird ihnen eine Liste von Gefährdungen zugeordnet. Dies wird in Form von Tabellen für jedes betrachtete Zielobjekt vermerkt, wobei der Schutzbedarf in den drei Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit ermittelt wird. Durch diese Tabellen kann ein Überblick über die Gefährdungslage gewonnen werden. Dieser Überblick wird anschließend mit zusätzlichen Gefährdungen der Zielobjekte erweitert. Als nächstes wird jedes Zielobjekt dahingehend überprüft, ob die Sicherheitsmaßnahmen, die bereits umgesetzt oder gemäß dem Sicherheitskonzept vorgesehenen sind, ausreichen. Ergibt die Gefährdungsbewertung, dass einige Maßnahmen nicht ausreichend sind, müssen zusätzliche Maßnahmen zur Behandlung der Risiken eingeführt werden. Falls bei der Behandlung von verbleibenden Gefährdungen ergänzende Maßnahmen zu den Standard-Sicherheitsmaßnahmen hinzugefügt wurden, muss das Sicherheitskonzept anschließend konsolidiert werden [BSI03, S. 21]. Danach kann die Vorgehensweise, wie im IT-Grundschutz beschrieben, fortgeführt werden.

3.3 Theoretische Grundlagen der Threat, Vulnerability and Risk Analysis TVRA

Vorab ist festzustellen, dass die TVRA-Methode keine Informationen über die Herstellung von Sicherheitstests enthält. Die Methode ist laut Spezifikation auf

Informations- und Kommunikationstechnologien anzuwenden und auf Basis der TVRA können die analysierten Telekommunikationssysteme evaluiert werden. Die Methode wurde hauptsächlich zur Sicherheitsstandardisierung entwickelt und berücksichtigt nur technische Verwundbarkeiten und Gegenmaßnahmen. Die geschäftlichen Auswirkungen bei der Verletzung der Sicherheit, werden wie gewöhnlich bei Standards nicht betrachtet [Mo11].

Die Literaturrecherche über die Methode erfolgte über Google Scholar und über den Online-Katalog der Universitätsbibliothek der Fernuni in Hagen. Des Weiteren wurde über den Online Katalog des DLR und dessen verfügbaren Zeitschriften Recherche von Elsevier - ScienceDirect Online-Journals, Springer Online-Journals, Wiley Online Library, Nature Publications, IEEE Journals/Proceedings, ACM Digital Library - Association for Computing Machinery nach den Kriterien *Threat, Vulnerability and Risk Analysis*, *Risikoanalyse*, *risk analysis* und *risk assessment* gesucht.

Als Ergebnis dieser Recherche wurde festgestellt, dass keine einschlägige Sekundärliteratur über die Threat, Vulnerability and Risk Analysis verfügbar ist. Dies kann auf mangelnde praktische Relevanz hinweisen, jedoch gibt es einige Veröffentlichungen ([Mo09], [WaLi09], [Re12], [Mo12], [KOJ12], [Bo15], [ET15]) bei denen die Methode auf bestimmte Anwendungsgebiete angepasst und angewendet wurde.

In ihrer Veröffentlichung „eTVRA, a Threat, Vulnerability and Risk Assessment Tool for eEurope" von Judith E. Y. Rossebø, Scott Cadzow und Paul Sijben [RCS07] wird herausgestellt, wie wichtig Standardisierung zur Sicherung für ein Netz der nächsten Generation ist, um Vertrauen in ihre Dienste und Infrastruktur aufzubauen und somit die Entwicklung moderner öffentlicher Dienstleistungen zu ermöglichen. Die Protokolle, die bei den NGN benutzt werden, wurden ursprünglich für Local Area Network (LAN) entwickelt und nur innerhalb von vertrauensvollen Bereichen mit vertrauensvollen Benutzern eingesetzt. Beim NGN werden diese Protokolle jedoch innerhalb des Internets, einem nicht vertrauensvollen Bereich mit nicht vertrauensvollen Nutzern, eingesetzt. Ein Standard, der Verwendet wird, um die Angriffe auf ein NGN zu analysieren, ist die TVRA. (Vgl. [RCS07]).

Zur Unterstützung für die Bewertung der Sicherheit eines IT-Produktes hat das ETSI eine Bedrohungs-, Schwachstellen- und Risikoanalyse (TVRA) für die Domäne der Telekommunikation (TelCo) entwickelt. Die TVRA-Methode baut auf der

Sicherheitsrisikoanalyse CORAS auf und ist so strukturiert, dass ihre Ausgabe direkt für eine Evaluierung gemäß den CC verwendet werden kann. (Vgl. [Mo09]).

CORAS ist eine modell-basierte Risikoanalysemethode, die aus acht Schritten besteht. Die ersten vier Schritte werden durchgeführt, um ein gemeinsames Verständnis über das Ziel der Analyse zu schaffen. Diese Zielbeschreibung dient als Grundlage für die nachfolgende Risikoidentifikation. Die vier einleitenden Schritte umfassen die Dokumentation, Annahmen über die Umgebung oder die Umgebung in der das System arbeiten soll, sowie einer vollständigen Liste, auf welche Aspekte besonders viel Aufmerksamkeit gelenkt werden soll und welche Aspekte ignoriert werden können. Die letzten vier Schritte sind der tatsächlichen Analyse gewidmet. Das beinhaltet die Identifizierung konkreter Risiken und ihr Schadensausmaß sowie die Aufstellung von Gegenmaßnahmen für die inakzeptablen Risiken. (Vgl. [LSS11], Kapitel 3)

Die TVRA basiert auf dem Risikomanagement Prozess von CORAS, der vom ETSI weiter entwickelt wurde [Mo09]. Um Beziehungen innerhalb des Systems zu modellieren, wird in der TVRA die Unified Modelling Language (UML) verwendet [ETS11].

Der Zweck der TVRA ist es, zu bestimmen, wie leicht angreifbar ein System oder die Systemkomponenten sind. Dies kann durch das Angriffspotential gemessen werden, welches sich aus den Faktoren Erfahrung, Verfügbarkeit/Möglichkeit und Ressource zusammensetzt ([ETS11], S. 15). Der Schlüssel für eine erfolgreiche TVRA ist die Fähigkeit die Beziehung zwischen den Schutzzielen und den Anforderungen des Systems darzustellen. So ist ein weiteres Anliegen der TVRA sicherzustellen, dass das Design des Systems selbst robust ist und hierfür komplett dokumentierte Anforderungen für all seine Systemaspekte existieren. Die TVRA verlangt, dass sowohl das zu untersuchende System wie auch die schützenswerten Güter des Systems und die Einbindung des Systems in seine Umgebung klar identifiziert sind. Eine wichtige Beziehung in der TVRA ist die Beziehung zwischen dem schützenswerten Gut und der Schadenanfälligkeit, welches als Risiko für dieses schützenswerte Gut bewertet wird [ETS11].

Die Methode führt ein systematisches Identifizieren der Störfälle, denen vorgebeugt werden soll, durch. Zusätzlich werden die schützenswerten Güter, aus denen das System aufgebaut ist, und ihre Schwachstellen identifiziert. Die Bedrohungen und die Bedrohungsfaktoren werden ebenfalls bestimmt. Bevor das Risiko für das System

bestimmt wird, werden die Wahrscheinlichkeit und das Ausmaß des Ausnutzens einer Schwachstelle beschrieben. Ein wichtiger Punkt der TVRA-Methode sind die Gegenmaßnahmen, die das System gegen Bedrohungen der Schadenanfälligkeit schützen und somit das Risiko vermindern sollen. In der technischen Spezifikation [ETS11] werden zwei Strategien für die Gegenmaßnahmen genannt. Dies ist zum einen die Neugestaltung des Systems und zum anderen, das bestehende System robuster zu machen.

Die TVRA beruht demnach auf Schwachstellenanalysen (vulnerabilitiy analysis). Bei einer Schwachstellenanalyse werden die Schwachstellen überprüft, die durch Bedrohungen ausgenutzt werden können. Hierbei müssen die bereits existierenden Schutzmaßnahmen und das Umfeld einbezogen werden. Von großer Bedeutung ist die Bewertung der Möglichkeit, eine Schwachstelle auszunutzen.

Die TVRA soll zyklisch wiederholt werden, sobald Änderungen von außen oder von innen aufgetreten sind, die durch den Einsatz von Gegenmaßnahmen hervorgerufen werden (siehe Tabelle 3-2 zyklische Natur der TVRA [ETS11, S. 15]).

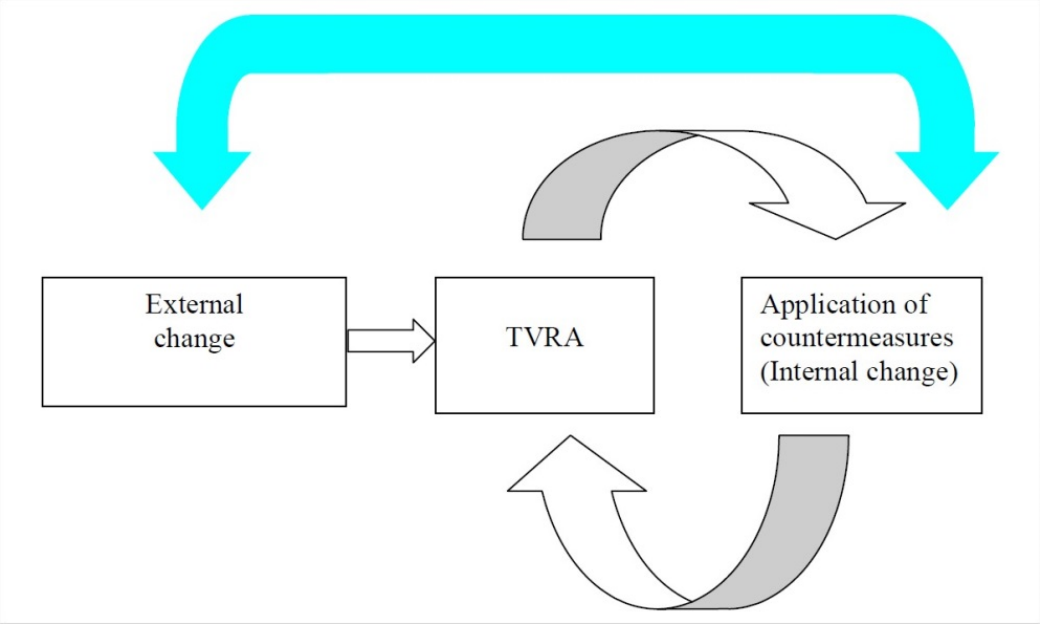

Tabelle 3-2 zyklische Natur der TVRA [ETS11, S. 15]

Die Methode ist an den CC angelehnt, wobei es kleine Unterschiede bei der Schwachstellenanalyse gemäß ISO/IEC 15408 und der TVRA gibt. Bei der finalen Evaluation nach CC wird davon ausgegangen, dass der Systementwurf abgeschlossen ist. Bei der TVRA werden erst die Schwachstellen identifiziert, die die Versorgung mit

Gegenmaßnahmen benötigen. Dann werden empfehlenswerte Gegenmaßnahmen identifiziert und angewendet. Und erst anschließend wird das System bewertet. [ETS11]

Die Methode wurde für die Evaluierung von intelligenten Transportsystemen (ITS) verwendet [ET10]. ITS gehören in den Bereich der Telematik und aller Arten von Kommunikation in Fahrzeugen, zwischen Fahrzeugen (zum Beispiel Car-to-Car), sowie zwischen Fahrzeugen und festen Standorten (z.B. Car-to-Infrastructure). Allerdings sind die ITS nicht auf den Straßenverkehr beschränkt, sie beinhalten auch die Nutzung von Informations- und Kommunikationstechnologien (IKT) für Schienen-, Wasser- und Luftverkehr, einschließlich Navigationssystemen. In der Regel setzen die verschiedenen Arten von ITS auf Funkdienste für die Kommunikation und verwenden spezielle Technologien [ETS16]. In [Bo15] wird die TVRA neben der EVITA X (E-safety Vehicle InTrusion protected Applications) Methode, als eine der beiden Hauptanalysemethoden für intelligente Transportsysteme genannt. Weitere Veröffentlichungen wie [MO12] oder [KOY12] zum Thema intelligente Transportsysteme verwenden für die Risikoanalyse ebenfalls die TVRA. Die beiden Hauptanwendungsgebiete der TVRA sind demnach die Sicherheit von NGN und die Evaluierung von intelligenten Transportsystemen.

Das System wird bei der TVRA gemäß der für diese Arbeit verwendeten technischen Spezifikation ETSI TS 102 165-1 V4.3.2 (2011-1) [ETS11] in zehn Schritten untersucht. Diese Version ist eine Erweiterung der ursprünglichen TVRA, die nur sieben Schritte einbezieht. Wie in [DR10] beschrieben, werden diese zehn Schritte linear, also hintereinander ausgeführt. In [DR10] wird auch erwähnt, dass der neunte Schritt nicht über einen funktionalen optimalen Zustand entscheidet, aber es wird für ausgewählte Gegenmaßnahmen eine einfache Kosten-Nutzen-Analyse angeboten. Wie diese Kosten-Nutzen-Analyse durchgeführt wird, ist in der Spezifikation nicht beschrieben, was für die praktische Durchführung zu einer Herausforderung werden kann.

Die zehn Schritte werden in den folgenden Unterabschnitten näher beschrieben.

3.3.1 Bestimmung des Evaluationsgegenstandes

Um die TVRA erfolgreich durchzuführen, ist es wichtig, eine genaue Bestimmung des Anwendungsbereichs, des Verwendungszwecks und der Zielsetzung der Analyse zu bestimmen.

Die Identifizierung des Anwendungsbereiches ist notwendig, damit genau dieser bei der Analyse einbezogen wird. Die Identifizierung hilft, die Grenzen zwischen dem Evaluationsgegenstand (EVG) und der Umgebung des Evaluationsgegenstandes zu bestimmen.

In der Sicherheitsumgebung werden Annahmen über die Umgebung beschrieben, in der der EVG eingesetzt werden soll. Hierbei sollen die Auflagen an den Betrieb mitbeachtet werden.

Der Zweck der TVRA soll deutlich bestimmt werden, damit die bestehenden Risiken erkannt werden, um dann entsprechende Schutzmaßnahmen einzuleiten. Durch diese Zielsetzung soll die Grundlage der TVRA klar ersichtlich sein.

3.3.2 Identifikation der Schutzziele

Bei der TVRA stehen vor allem die Schutzziele im Vordergrund, die beim Nutzen von Telekommunikationsdiensten sichergestellt werden sollen:

- der Schutz der Privatsphäre und der personenbezogenen Daten
- die Sicherstellung der fortlaufenden und ordnungsmäßigen Verfügbarkeit der Telekommunikationsdienste
- der Schutz gegen Missbrauch

Gemäß der Spezifikation gibt es bei der TVRA vier Bedrohungskategorien gegen ein Kommunikationssystem (vgl. 2.5.1). Diese werden in der Tabelle 3-3 Bedrohungskategorien und ihre Schutzziele [ETS11, S. 17] gegenübergestellt.

Bedrohungskategorie	**Sicherheitseigenschaft/Schutzziel**
Abhören von Daten (Interception)	Vertraulichkeit (Confidentiality)
Unbefugtes Ändern von Daten (Manipulation)	Integrität (Integrity)
Verhindern/unterbrechen der Kommunikationsbeziehung (Denial	Verfügbarkeit (Availability)

of Service)	
Verleugnung der Teilnahme an einer Kommunikation (Repudiation) durch den Sender oder den Empfänger	Abrechenbarkeit (Accountability)Authentizität/Nachweisbarkeit (Authenticity)

Tabelle 3-3 Bedrohungskategorien und ihre Schutzziele [ETS11, S. 17]

Diese Schutzziele werden verwendet, um die funktionalen Sicherheitsanforderungen abzuleiten.

3.3.3 Identifikation der funktionalen Sicherheitsanforderungen

Die Sicherheitsanforderungen beschreiben wie Sicherheitsziele erreicht werden. Sie lassen sich in zwei Bereiche unterteilen: Dies sind zum einen die funktionalen Sicherheitsanforderungen und zum anderen die Sicherheitsanforderungen der Vertrauenswürdigkeit. Für die Identifikation der funktionalen Anforderungen enthält Teil 2 der CC [CC02] modulare Anforderungskomponenten. Die Sicherheitsanforderungen der Vertrauenswürdigkeit werden im Teil 3 der CC [CC03] beschrieben, der wiederum modulare Anforderungskomponenten enthält.

3.3.4 Systematische Bestandsaufnahme aller Assets

Alle schützenswerten Güter des Systems, die Komplexität der Technologie, die bei der Herstellung der schützenswerten Güter verwendet wurde und alle Informationen zur Technologie des schützenswerten Gutes, die öffentlich zur Verfügung stehen, müssen dokumentiert werden. Es gibt drei Arten von schützenswerten Gütern:

- die physikalischen (IT-Systeme, Daten)
- die menschlichen (Personen) und
- die logischen (Prozesse)

[RCS07].

Um diese schützenswerten Güter zu erhalten, werden typische Szenarien des Systems durchgespielt. Eine Datenbank kann bei der Dokumentation der gefundenen schützenswerten Güter und ihren Beziehungen zu anderen schützenswerten Gütern oder zum System behilflich sein.

Die exakte Bestimmung des Schadensausmaßes auf ein schützenswertes Gut ist nicht möglich. Deswegen werden qualitative Skalen für seine Beschreibung verwendet. Bei

der TVRA werden die Stufen niedrig, mittel und hoch verwendet. Siehe Tabelle 3-4 Stufen des Schadensausmaßes eines schützenswerten Gutes (vgl. [ETS11], S. 31):

Wert Schadensausmaß	**Kurzbeschreibung Schadensausmaß**	**Ausführliche Beschreibung Schadensausmaß**
1	Niedrig	Der betroffene Teil ist nicht sehr stark beschädigt, der mögliche Schaden ist gering
2	Mittel	Die Bedrohung richtet sich an das Interesse der Anbieter / Teilnehmer und kann nicht vernachlässigt werden
3	Hoch	Eine Geschäftsgrundlage ist bedroht und schwere Schäden könnten in diesem Zusammenhang auftreten

Tabelle 3-4 Stufen des Schadensausmaßes eines schützenswerten Gutes (vgl. [ETS11], S. 31)

3.3.5 Systematische Identifikation der Verwundbarkeiten

Für die Identifikation der Verwundbarkeiten müssen zuerst die Schwachstellen des Evaluierungsgegenstandes und seiner Umgebung festgestellt werden. Anschließend werden Bedrohungen ermittelt, welche diese Schwachstellen ausnutzen und dem Evaluierungsgegenstand Schaden zufügen können. Erst wenn so eine Bedrohung existiert, wird diese Schwachstelle als Verwundbarkeit angesehen. Die Vorgehensweise in diesem Schritt der TVRA ist folgende:

a. Identifikation der Schwachstellen
b. Identifikation der Verwundbarkeiten - hierfür werden die möglichen Angriffe ermittelt
c. Identifikation der Angriffsmethoden - die Angriffsmethoden sind die Aktionen eines bestimmten Threat Agents (siehe 2.5)

Die Wahrscheinlichkeit, dass ein Angreifer einen erfolgreichen Angriff durchführen kann, hängt vom jeweiligen Angriffspotential ab. Für die Bewertung der Angriffsschwierigkeit wird bei der TVRA das Angriffspotential auf Basis der „Common Methodology for Information Technology Security Evaluation“ [CEM01] bewertet. Das Angriffspotential hängt von mehreren Faktoren ab:

(1) Benötigte Zeit, um Schwachstellen zu finden und auszunutzen

(2) Benötigter Grad an Expertise

(3) Benötigtes Wissen über das System

(4) Benötigter Zugriff auf das System

(5) Benötigte Hardware/Software für die Analyse bzw. Ausnutzung

Für jeden dieser Faktoren sind bestimmte Kategorien festgelegt, die mit Werten hinterlegt sind.

Faktor	**Kategorien**	**Wert**
Zeit	≤ 1 Tag ≤ 1 Woche ≤ 1 Monat ≤ 3 Monate ≤ 6 Monate > 6 Monate	0 1 4 13 26 Es besteht akutes Angriffspotential
Expertise	Laie Profi Experte	0 2 5
Wissen	öffentlich begrenzt sensitiv kritisch	0 1 4 10
Zugriff	unbegrenzt einfach moderat schwer keiner	0 1 4 12 Angriff kann nicht ausgeführt werden
Ausrüstung	Standard Speziell Maßgeschneidert	0 3 7

Tabelle 3-5 Abbildung der Kategorien der einzelnen Faktoren und ihre zugehörigen Werte (vgl. [ETS11], S. 36)

Für jeden Angriff ordnet ein Sicherheitsfachmann jedem dieser 5 Faktoren eine Kategorie zu. Da die Eingruppierung eine bestimmte Begründung voraussetzt, ist diese Einordnung von anderen Personen nachzuvollziehen. Die Einordnung kann nach Einbeziehung anderer Begründungen abgeändert werden.

Ein weiterer Faktor, um das resultierende Gesamtausmaß des Angriffs zu berechnen, ist der Angriffsintensitätsfaktor. Es gibt drei Intensitätslevel:

- eine einzige Angriffsgelegenheit
- eine mäßige Anzahl von Angriffsgelegenheiten
- eine große Anzahl von Angriffsgelegenheiten

Die Veränderung der Angriffsintensität kann entweder durch die Anzahl der Angriffe, die Erhöhung der Zeitspanne zwischen zwei Angriffen oder durch eine Kombination von beiden erreicht werden.

3.3.6 Berechnung der Eintrittswahrscheinlichkeit eines Angriffes und seine Auswirkungen

Die exakte Bestimmung der Eintrittswahrscheinlichkeit ist im Allgemeinen nicht möglich. Deswegen werden qualitative Skalen für seine Beschreibung verwendet. Bei der TVRA werden die Stufen *unwahrscheinlich, möglich* und *wahrscheinlich* verwendet.

Für die Bestimmung der Risikozahlen werden quantitative Zahlen für die entsprechenden qualitativen Skalen der Wahrscheinlichkeit verwendet.

Für die Berechnung des Angriffspotentials werden die einzelnen Werte für jeden Faktor, die im vorherigen Schritt bestimmt wurden, aufsummiert. Das Angriffspotential dieses Angriffes wird so als einzelne Zahl darstellbar. Es entstehen unterschiedliche Angriffspotentiale, die von akuter Angriffsgefahr, über hoher, mäßiger, normaler bis zu keiner Bewertung der Angriffsgefahr abgebildet werden. Die Abbildung der berechneten Werte des Angriffspotentials auf die entsprechende Angriffsgefahr befindet sich in der Tabelle 3-6 Abbildung der Werte des Angriffspotentials auf die Angriffsgefahr(vgl. [ETS11], S. 36)

Angriffspotential	**Angriffsgefahr**
0 bis 2	Keine Bewertung
3 bis 6	Normale
7 bis 14	Mäßige
15 bis 26	Hohe
> 26	Akute

Tabelle 3-6 Abbildung der Werte des Angriffspotentials auf die Angriffsgefahr(vgl. [ETS11], S. 36)

Diese Angriffsgefahr wird auf die Eintrittswahrscheinlichkeit folgendermaßen abgebildet:

Angriffsgefahr	Eintrittswahrscheinlichkeit
Keine Bewertung	Wahrscheinlich
Normale	
Mäßige	Möglich
Hohe	Unwahrscheinlich
Akute	

Tabelle 3-7 Abbildung der Angriffsgefahr auf seine Eintrittswahrscheinlichkeit (vgl. [ETS11], S. 36)

3.3.7 Aufstellen der Risiken

Das Risiko wird in dem ETSI-Standard als Produkt der Eintrittswahrscheinlichkeit eines Angriffes und seines Gesamtschadensausmaßes definiert [ETS11].

Das Gesamtschadensausmaß berechnet sich aus dem Intensitätsfaktor des Angriffes und des Schadensausmaßes.

Der Intensitätsfaktor des Angriffes kann die Werte 0, 1 oder 2 annehmen [siehe.3.3.6].

Das Schadensausmaß auf den Asset kann die Werte 1,2 oder 3 für die entsprechenden qualitativen Skalen des Schadensausmaßes annehmen [vgl. 3.3.4].

Aus diesem Grund soll das Gesamtschadensausmaß ebenfalls nur die Werte 1, 2 oder 3 annehmen. Werte die durch die Addition des Intensitätsfaktors und des Schadensausmaßes des Asset einen Wert größer als 3 ergeben, erhalten daher auch den Wert 3.

Für die Eintrittswahrscheinlichkeit können bei ETSI die Werte 1, 2 oder 3 für die entsprechenden qualitativen Skalen der Wahrscheinlichkeit auftreten [siehe 3.3.6].

Somit sind die möglichen Werte für das Risiko, welches aus dem Produkt der Wahrscheinlichkeit und seines Gesamtschadensausmaßes berechnet wird, 1,2, 3,4, 6 und 9. Die Werte 5,7 und 8 können nicht auftreten. Diese Risikowerte und ihre Beschreibung finden sich in der Tabelle 3-8 Risikowerte und ihre Erläuterungen wieder.

Risikowert	Erklärung
[1,2]	Geringes Risiko: es besteht keine Notwendigkeit Gegenmaßnahmen anzuwenden.
[3,4]	Großes Risiko: es ist wahrscheinlich, dass das Risiko eintritt aber dies wäre nicht fatal; Gegenmaßnahmen sollten angewendet werden.
[6, 9]	Kritisches Risiko: Risiko sollte mit der höchsten Priorität verringert werden.

Tabelle 3-8 Risikowerte und ihre Erläuterungen

3.3.8 Identifikation von Sicherheits-Gegenmaßnahmen

Ziel von Sicherheits-Gegenmaßnahmen ist entweder die Eintrittswahrscheinlichkeit oder das Schadensausmaß eines Angriffes zu verringern. Zunächst einmal müssen die möglichen Gegenmaßnahmen identifiziert werden. Im nächsten Schritt kann eine Kosten-Nutzen-Analyse der Gegenmaßnahmen bestimmt werden, deren Einsatz (der Nutzen) den Aufwand (die Kosten) rechtfertigt. Zu beachten ist, dass auch Gegenmaßnahmen ihre eigenen Verwundbarkeiten besitzen.

Es können mehrere Gegenmaßnahmen zum Schutz von einem Asset benötigt werden. Sie können durch Inspektion und Erfahrung ermittelt werden. Es existieren Organisationen, wie das CERT (Computer Emergency Response Team), die bekannte Schwachstellen sammeln. Leider dauert es eine gewisse Zeit, bis neue Schwachstellen und die Möglichkeiten zur Beseitigung dieser, bereitgestellt werden. Deswegen sind entsprechende Veröffentlichungen der Hersteller auf ihren Internetseiten eine weitere Möglichkeit für die Gewinnung von Gegenmaßnahmen.

Durch den Einsatz von Gegenmaßnahmen muss die Auswirkung des Angriffes neu berechnet werden [ETS11]. Es werden bei der TVRA nur technische Sicherheitsmaßnahmen betrachtet (vgl. [ETS11, S. 27]). Unter technischen Maßnahmen sind gemäß [BFD16] alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind, wie etwa

- Umzäunung des Geländes
- Sicherung von Türen und Fenstern
- Bauliche Maßnahmen allgemein

- Alarmanlagen jeglicher Art

oder Maßnahmen die in Soft- und Hardware umgesetzt werden, wie etwa

- Benutzerkonto
- Passworterzwingung
- Logging (Protokolldateien)
- Biometrische Benutzeridentifikation

Siehe Bundesdatenschutzgesetz (BDSG) § 9 Technische und organisatorische Maßnahmen, sowie § 9 Satz 1 Anlage.

Der IT-Grundschutz-Katalog vom Bundesamt für Sicherheit in der Informationstechnik (BSI) mit seinen Maßnahmenkatalogen bietet eine gute Grundlage für die Identifikation unterschiedlicher Gegenmaßnahmen.

3.3.9 Kosten-Nutzen-Analyse der Gegenmaßnahmen

In diesem Schritt soll aus den Alternativen der Gegenmaßnahmen die kosteneffektivste Gegenmaßnahme identifiziert werden. Bei den Kosten handelt es sich nicht nur um finanzielle Aspekte, sondern sie beeinflussen auch den Entwurf, die Umsetzung und den Betrieb. Für die Kosten-Nutzen-Analyse stellt die TVRA-Methode Bewertungstabellen für die Bereiche Entwurf, Umsetzung, Betrieb, Ausmaß auf Anforderungen von Behörden und Marktakzeptanz zur Verfügung. Anhand dieser Tabellen soll der Einfluss der Gegenmaßnahmen auf diesen Bereich angegeben werden. Als Ergebnis erhält man einen Zahlenwert. Ist der Zahlenwert gleich 0 bedeutet dies, die Gegenmaßnahme hat keinen Einfluss. Bei einem negativen Wert hat die Gegenmaßnahme einen negativen Einfluss, bei einem positiven Wert ist der Einfluss der Gegenmaßnahme positiv.

3.3.10 Spezifikation von detaillierten Anforderungen

Meistens sind die Sicherheitsanforderungen ausreichend, die sich aus dem Schritt 3 (*Identifikation der funktionalen Sicherheitsanforderungen*) und den Schritten 8 (*Identifikation von Sicherheitsgegenmaßnahmen*) und 9 (*Kosten-und Nutzen-Analyse der Gegenmaßnahmen*) ergeben. Allerdings kann es auch vorkommen, dass detaillierte Anforderungen nicht direkt aus den bestehenden Standards und internationalen Spezifikationen abgeleitet werden können [ETS08, S.16], dann müssen komplett neue Sicherheitsanforderungen definiert werden. Diese Definition von detaillierten Anforderungen soll in diesem Schritt durchgeführt werden.

Durch den Einsatz der TVRA soll ein angemessenes Sicherheitsniveau erreicht werden. Als Ziel hat sie den Aufbau eines sicheren Designs des IT-Systems zu unterstützen. Die Durchführung einer TVRA ist eine kritische Analyse eines Systems. Mit ihrer Hilfe können Fehler im Design des Systems identifiziert und ggfs. korrigiert werden, um die System- und Sicherheitsziele zu erreichen. Die Ergebnisse der Analyse können als Nachweis für die Qualität eines evaluierten Systems benutzt werden.

4 Anwendung der TVRA auf ein hochwertiges Erdfernerkundungssystem

Ein Erdfernerkundungssystem ist ein sehr komplexes System, siehe Abbildung 4-1 Übersicht der Komponenten eines Erdfernerkundungssystems. Hier wird ein Erdfernerkundungssystem mit einem Radarsatelliten abgebildet.

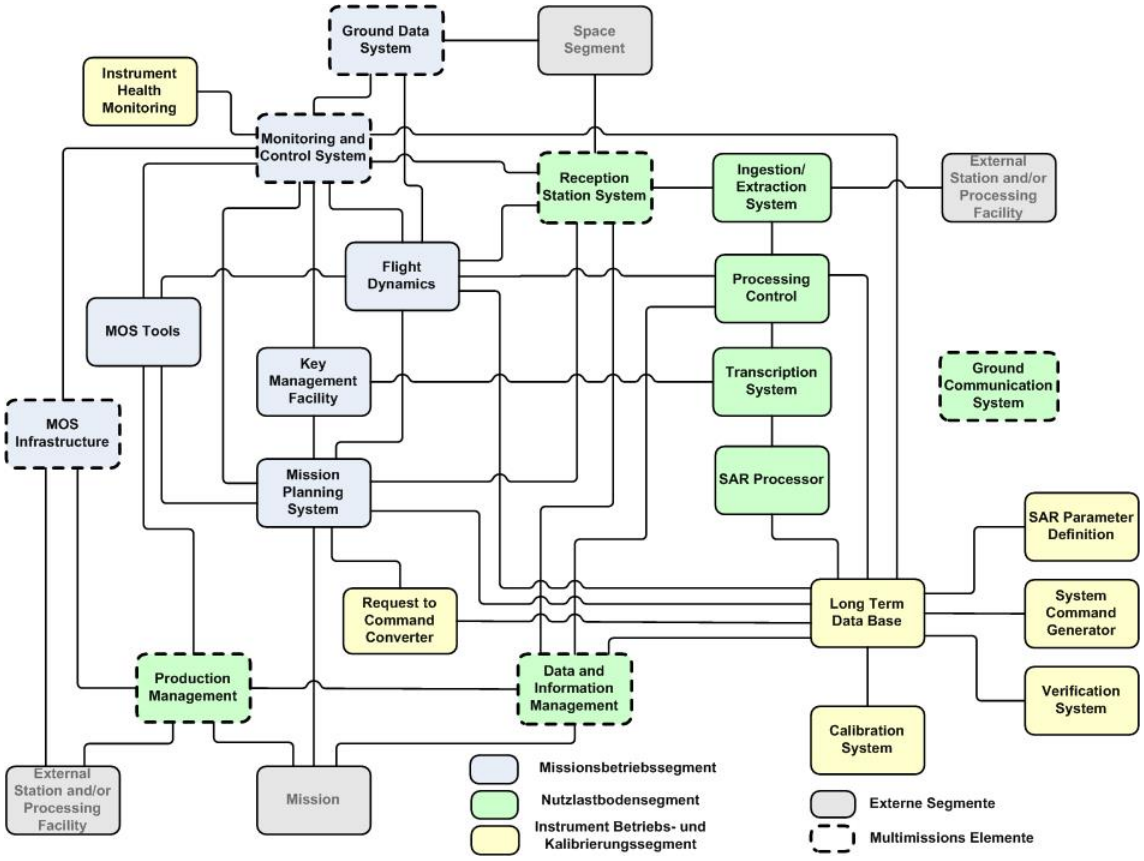

Abbildung 4-1 Übersicht der Komponenten eines Erdfernerkundungssystems

Eine detaillierte Analyse des Gesamtsystems ist im Rahmen einer Masterarbeit nicht machbar. Um ausreichende Informationen über die Anwendung der Methode zu erhalten, wird die Methode auf drei Teilsysteme des Gesamtsystems angewendet.

Es werden die Teilsysteme Bodenstation (Receiving Station System), Transkription Prozessierungssystem (Transcription System) und eine webbasierte Benutzerschnittstelle (innerhalb des Daten- und Informationsmanagements) für die Anwendung der Risikoanalysemethode TVRA verwendet.

Die Bodenstation ist für den Empfang und die Weiterleitung der Erdfernerkundungsdaten zuständig.

Das Transkription Prozessierungssystem (TSC) befindet sich an allen Bodenstationen, die bei einer höherwertigen Erdfernerkundungsmission beteiligt sind. Es ist für die Entschlüsselung der empfangenen Erdfernerkundungsdaten zuständig.

Die webbasierte Nutzerschnittstelle ermöglicht den Zugang zu den Erdbeobachtungsdaten und ist somit Teil des Daten- und Informationsmanagementsystems (DIMS). Diese Benutzerschnittstelle wird für die Suche, Bestellung und Auslieferung von Erdfernerkundungsdaten benötigt.

Einen Ausschnitt der Teilkomponenten, an denen die Methode angewendet wird, zeigt die Abbildung 4-2 Ausschnitt der Teilkomponenten:

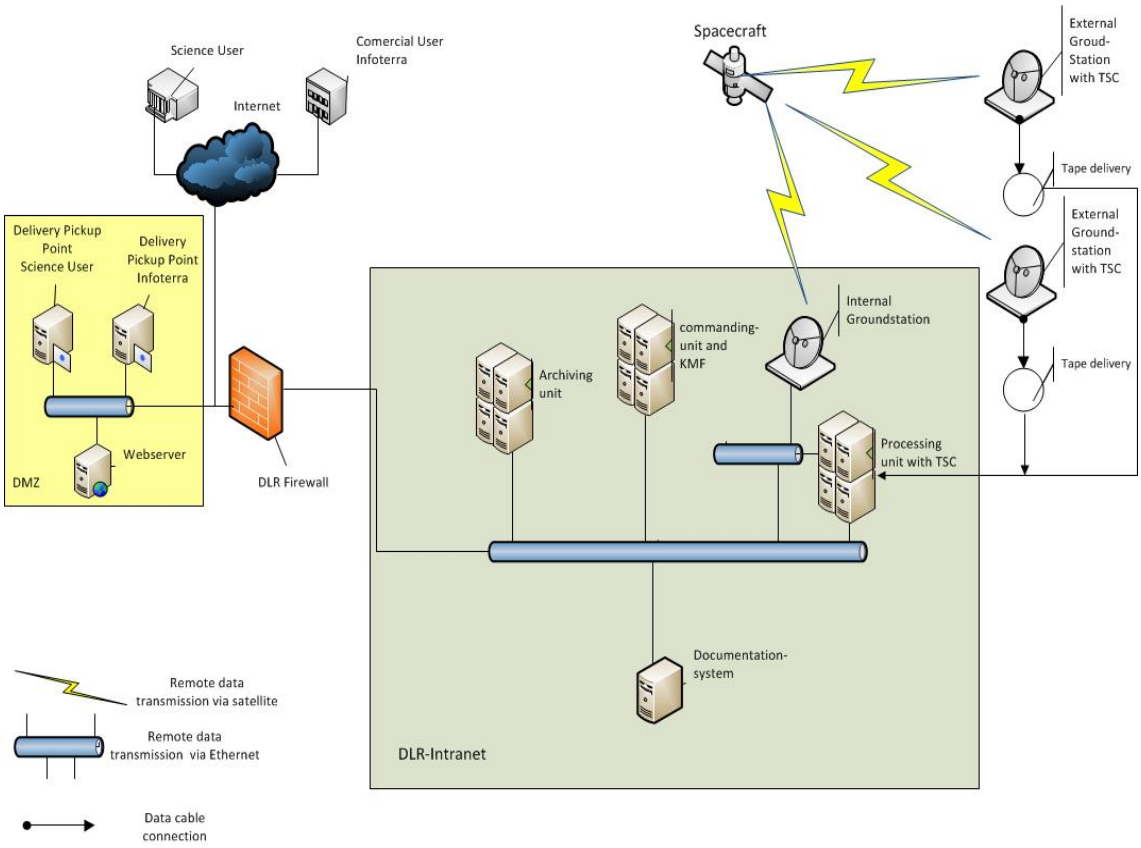

Abbildung 4-2 Ausschnitt der Teilkomponenten

Um mögliche unterschiedliche Angriffspunkte herauszustellen, wurden diese Teilkomponenten für die Anwendung der TVRA ausgewählt.

Die Teilkomponente Bodenstation wurde gewählt, um mögliche Schwachstellen aufzuzeigen, die bei den satellitengestützten Datentransfers existieren. Wie in der Abbildung 4-2 Ausschnitt der Teilkomponenten zu erkennen, wird für die Datenfernübertragung ein Satellit und eine Antenne einer Bodenstation benötigt.

Das Transkription Prozessierungssystem befindet sich innerhalb des DLR-Intranetzes. Die Angriffsmöglichkeiten sollten hierbei auf eigene Mitarbeiter mit eingeschränkten bzw. privilegierten Zugriffsrechten und fremden Mitarbeiten mit eingeschränkten Zugriffsrechten begrenzt sein. Ein Angreifer ohne Zugriffsrechte benötigt sowohl erhebliche Fachkenntnisse als auch die Mitarbeit eines fachkundigen Innentäters.

Im Gegensatz dazu ist die webbasierte Nutzerschnittstelle die am stärksten exponierte Teilkomponente, da der Informationsaustausch vorwiegend über das Internet getätigt wird. Die drei Teilkomponenten werden im nächsten Abschnitt näher beschrieben.

Die systematische Identifikation der Schwachstellen, Verwundbarkeiten, Bedrohungen und der Angriffsmethoden wurden mit der Unterstützung von Experten ermittelt. Das System zur Erfassung der TVRA-Datenbank basiert auf einem sogenannten LAMP-System. Die Akronyme stehen für L = Linux (das Betriebssystem), A = Apache (der Webserver), M = MySQL (das Datenbankverwaltungssystem) und P = Perl (die verwendete Programmiersprache). Darüber hinaus wurde für die Oberflächengestaltung die JavaScript-Bibliothek Dojo-Toolkit verwendet.

4.1 Bodenstation

Anhand der Bodenstation in Neustrelitz (RS-NSG) wird die Anwendung der TVRA-Methode näher betrachtet. Hierfür wird das Design-Dokument [DLR02] der Bodenstation in Neustrelitz aus der TanDEM-X Mission als Informationsgrundlage verwendet.

Bestimmung des Evaluationsgegenstandes

Um den Evaluierungsgegenstand zu bestimmen, werden im Folgenden die einzelnen Komponenten des Teilsystems und der Datenfluss für den Datenempfang detailliert beschrieben. Dadurch sollen zum einen die Identifikation der schützenswerten Güter im nächsten Schritt erleichtert werden und die Angriffspunkte innerhalb des betrachteten Teilsystems leichter erkannt werden.

Die Bodenstation in Neustrelitz (RS-NSG) empfängt innerhalb ihres Sichtbarkeitsbereiches Daten von einem Satelliten. Der Satellit, eine Teilkomponente des Erdfernerkundungssystems, liefert die SAR-Daten für die weiteren Verarbeitungsschritte an das Transkription Prozessierungssystem und den TerraSAR-Multimode SAR-Prozessor (TMSP).

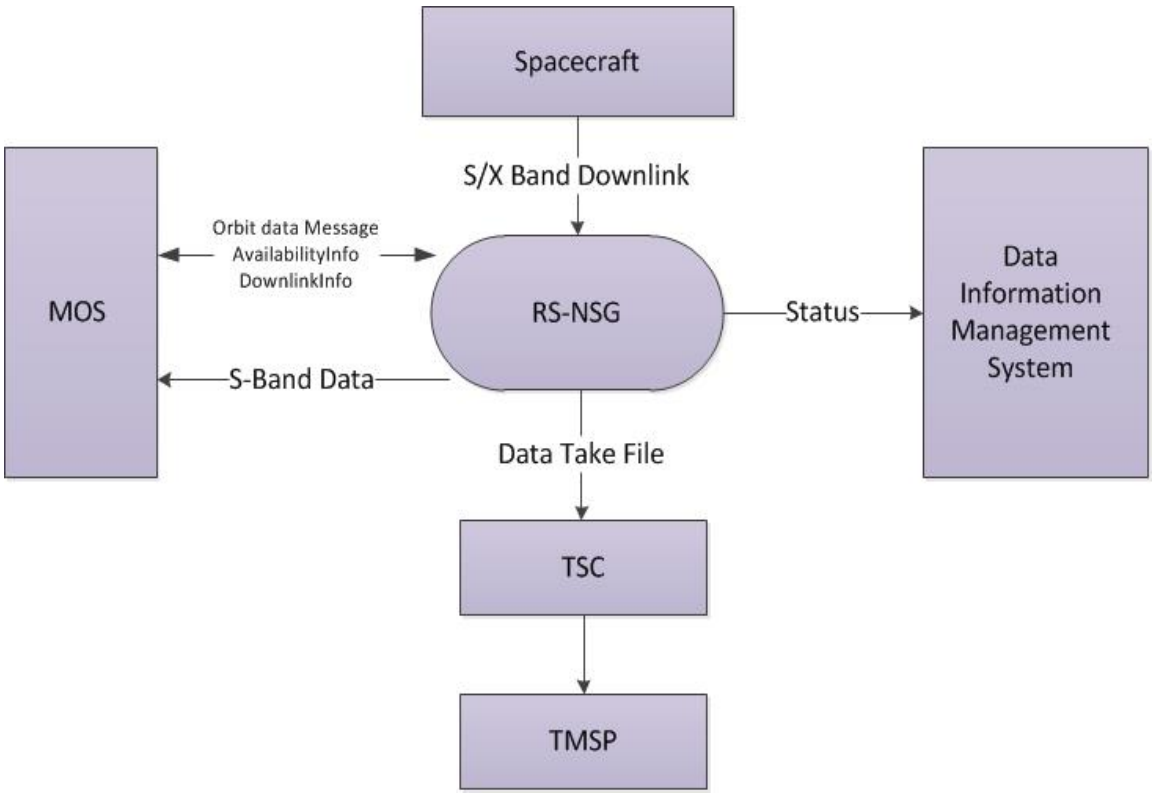

Abbildung 4-3 Datenfluss für den Datenempfang von SAR-Daten an der Bodenstation Neustrelitz [DLR02]

Innerhalb des Erdfernerkundungssystems gibt es mehrere Bodenstationen, die auf der Welt verteilt sind, um den Empfang der Daten weltweit zu ermöglichen und die Speicherkapazität und die Verfügbarkeit des Satelliten optimal auszunutzen.

Alle TanDEM-X Downlinks werden bereits ein bis zwei Wochen im Voraus an der Bodenstation eingeplant. Anhand einer Verfügbarkeitsdatei können alle Satelliten, die den Sichtbarkeitskreises der Bodenstation überfliegen, abgefragt werden, so dass sehr früh mögliche Konflikte erkannt werden können. Dies dient zur Unterstützung für das Missionsbetriebssegment (MOS), um den Datenempfang mit einem hohen Maß an Zuverlässigkeit zu planen. Der Empfang der Daten basiert auf der Downlinkinfo-Datei und den Satellitenbahnelementen, die von dem Missionsbetrieb bereitgestellt werden. Die empfangenen TanDEM-X Nutzdaten werden im TDX-Empfänger demoduliert, bit-synchronisiert und kodiert. Dieser Datenstrom aus dem TDX–Empfänger wird an das Direkt Archivsystem (DAS) übertragen und dort in einem aus Festplatten bestehenden RAID gespeichert.

Der Status über die Empfangsergebnisse wird dem Daten- und Informationsmanagementsystem (DIMS) mitgeteilt. Die Übertragung wird über das Campus-Netzwerk des DLR realisiert. Ein Campus-Netzwerk ist ein Netzwerk, welches

sich auf einen bestimmten geographischen Bereich bezieht und lokale Netzwerke miteinander verbindet. Hierbei werden nicht die öffentlichen Fernmeldebereiche verwendet. Gemäß dem §4 (1) Nr. 3 des SatDSiG [BJV07] müssen die Daten, die von dem Satelliten zur Bodenstation übermittelt werden, gegen unbefugte Kenntnisnahme geschützt werden.

In dem Evaluierungsgegenstand sind die Komponenten Satellit, Missionsbetrieb, Daten- und Informationsmanagementsystem und weiterverarbeitende Komponenten, wie das TSC und der TMSP, nicht enthalten. Das TSC und ein Teil des Daten-Informationsmanagementsystems werden in den nachfolgenden Unterabschnitten (4.2 und 4.3) näher betrachtet.

Identifikation der Schutzziele

Für die Identifikation der Schutzziele wurde der EVG auf die TVRA-relevanten Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Abrechenbarkeit bzw. Nachweisbarkeit) untersucht. Durch den vorherigen Schritt („Bestimmung des EVG“) wurde eine Übersicht des Systems dargestellt. Die durch Inspektion des Systems identifizierten Schutzziele sind im Annex A1 gelistet. Das Schutzziel Abrechenbarkeit bzw. Nachweisbarkeit spielt im Zusammenhang mit der Bodenstation keine Rolle.

Identifikation der funktionalen Sicherheitsanforderungen

Im Teil 2 der CC sind die funktionalen Sicherheitsanforderungen für Informationssysteme sehr vollständig beschrieben. Dies hat zum einen den Vorteil, dass sie weit verbreitet angewendet werden können, jedoch ist dies auch ein Nachteil, wenn nur einige Schutzziele betrachtet werden sollen, wie es bei der TVRA der Fall ist. Für die Analyse müssen alle funktionalen Sicherheitsanforderungen aus dem umfangreichen Katalog untersucht werden und aus diesen die geeigneten ausgewählt werden. Diese Analyse ist sehr zeitaufwendig. Deswegen wurden zuerst die Klassen der funktionalen Sicherheitsanforderungen betrachtet und aus diesen, die für den Evaluierungsgegenstand relevanten Komponenten ermittelt. Für den Evaluierungsgegenstand Bodenstation wurden die Klassen „Schutz der Benutzerdaten“ und „Identifikation und Authentisierung“ als relevant betrachtet. Die Auflistung der funktionalen Sicherheitsanforderungen findet sich im Annex A1.

Systematische Bestandsaufnahme aller Assets (schützenswerte Güter)

Für die Bestandsaufnahme aller Assets wurden die einzelnen Systembestandteile, vor allem in Bezug auf Telekommunikation, betrachtet und folgende schützenswerte Güter identifiziert:

- X-Band Daten = Radardaten (logische schützenswerte Güter)
- Empfangsausrüstung (physikalische schützenswerte Güter)
- Antenne (physikalische schützenswerte Güter)

Menschliche schützenswerte Güter wurden nicht betrachtet.

Diese schützenswerten Güter sind im TVRA-Datenbankmanagementsystem systematisch aufgenommen worden.

Systematische Identifikation der Verwundbarkeit

Für die Ermittlung der vorhandenen Schwachstellen bzw. Verwundbarkeiten und die Ermittlung der möglichen Angriffe wurde auf den Annex D der ISO/IEC 27005:2011 [ISO11] zurückgegriffen. Dieser Annex enthält eine Liste von Verwundbarkeiten bestimmter Sicherungsbereiche und gibt zusätzlich Beispiele für Bedrohungen an, die diese Verwundbarkeit ausnutzen können. Die Identifikation wurde gemäß technischer Spezifikation [ETS11, S. 32] in folgenden Schritten durchgeführt:

- Identifikation der Schwachstellen,
- Identifikation der Verwundbarkeiten, hierfür werden die möglichen Angriffe ermittelt,
- Identifikation der Angriffsmethoden.

Die Bestimmung der einzelnen Faktoren, um das Angriffspotential zu berechnen, hat sich als äußerst schwierig herausgestellt. Für die einzelnen Schritte wurden Experten des Systems zu Rate gezogen. Leider handelt es sich bei keinem dieser Mitarbeiter um einen Sicherheitsexperten. Wie die Schritte 3.3.6, 3.3.7 und 3.3.9 stellt sich die praktische Durchführung der Bestimmung der einzelnen Faktoren als ein sehr subjektiver Vorgang dar. Von einer vollständigen Liste kann nicht ausgegangen werden. Die Ergebnisse sind im Annex A1 zu finden.

Berechnung der Eintrittswahrscheinlichkeit eines Angriffes und seine Auswirkungen

Wie im Kapitel 3.3.6 beschrieben, werden für die Berechnung der Eintrittswahrscheinlichkeit eines Angriffes und seine Auswirkungen, die

Angriffsfaktoren für jeden Angriff benötigt. Die Bestimmung der genauen Werte für die einzelnen Faktoren wurde zusammen mit Projektmitarbeitern getätigt. Diese Mitarbeiter sind keine Sicherheitsexperten, besitzen aber Grundkenntnisse über Informationssicherheit und sind Experten für das zu betrachtende Teilsystem. Dieser Schritt wird für die Darstellung mit dem nächsten Schritt „Beschreiben der Risiken“ zusammengefasst.

Beschreiben der Risiken

Um das Risiko zu beschrieben werden die Risikowerte, wie in Kapitel 3.3.7 dargestellt, berechnet. Diese Werte werden anschließend gemäß der Abbildungstabelle aus 3.3.7 als ein qualitativer Wert angezeigt. Dieser Schritt hängt sehr stark von dem Fachwissen der Personen ab, welche die Analyse durchführen. Diese Personen sollten sowohl Detailwissen über das betrachtete System besitzen, wie auch spezielle Kenntnisse über IT-Sicherheit. Die Ergebnisse dieses Schrittes finden sich im Annex A2 *Risikoabschätzung* wieder.

Identifikation von Gegenmaßnahmen

Für die Identifikation der Gegenmaßnahmen wurde die technische Richtlinie des SatDSig [BSI07], welche auf dem IT-Grundschutzhandbuch [BSi08] basiert, zu Hilfe genommen. In dem IT-Grundschutzhandbuch werden Standardsicherheitsmaßnahmen für IT-Systeme beschrieben. Dieser Maßnahmenkatalog umfasst die Bereiche Infrastruktur, Organisation, Personal, Hardware und Software, Kommunikation und Notfallversorgung. Die Gegenmaßnahmen müssen immer im Zusammenhang mit einem identifizierten Risiko in Verbindung stehen. Die identifizierten Gegenmaßnahmen sind im Annex A1 aufgeführt.

Kosten-Nutzen-Analyse der Gegenmaßnahmen

Die Kosten-Nutzen-Analyse stellte sich als einer der schwierigsten Schritte bei der TVRA-Methode dar, da zum einen keine Erfahrungswerte existieren, auf die zurückgegriffen werden kann und zum anderen Mitarbeiter bei diesem Schritt zurate gezogen wurden, die sehr gute Fachkenntnisse über das System haben, aber keine Sicherheitsexperten sind. Die verfügbaren und befragten Sicherheitsexperten besitzen hingegen keine detaillierten Kenntnisse über das System und machten keine definitiven Aussagen. Aus diesem Grund sind die Ergebnisse, die in der TVRA-Datenbank

abgelegt wurden, als subjektiv zu betrachten. Siehe Annex A2 *Gegenmaßnahmen-Kosten-Nutzen-Tabelle*.

Spezifikation von detaillierten Anforderungen

Um die detaillierten Anforderungen zu identifizieren wurde das Dokument TanDEM-X / TerraSAR-X - Security Requirements and Data Policy Principles – [DLR08] untersucht und folgende detaillierten Anforderungen erkannt:

- Der S-Band Downlink soll nicht verschlüsselt werden.
- Das DLR hat die Kontrolle über den Daten-Downlink sicherzustellen.
- Personen, die Zugriff auf Ausrüstungen der Empfangsanlagen haben, müssen sich einer einfachen Sicherheitsüberprüfung (Ü1) unterziehen.

Weitere detaillierte Anforderungen wurden nicht erkannt.

4.2 Transkription Prozessierungssystem

Für die Analyse wurden die Dokumente *Transcription System Design Document* [DLR03] und das *Transcryption User Manual* [DLR04] zu Hilfe genommen.

Bestimmung des Evaluationsgegenstandes

Der Evaluierungsgegenstand schließt Hardware- und Softwarekomponenten ein und umfasst im Wesentlichen folgende Komponenten:

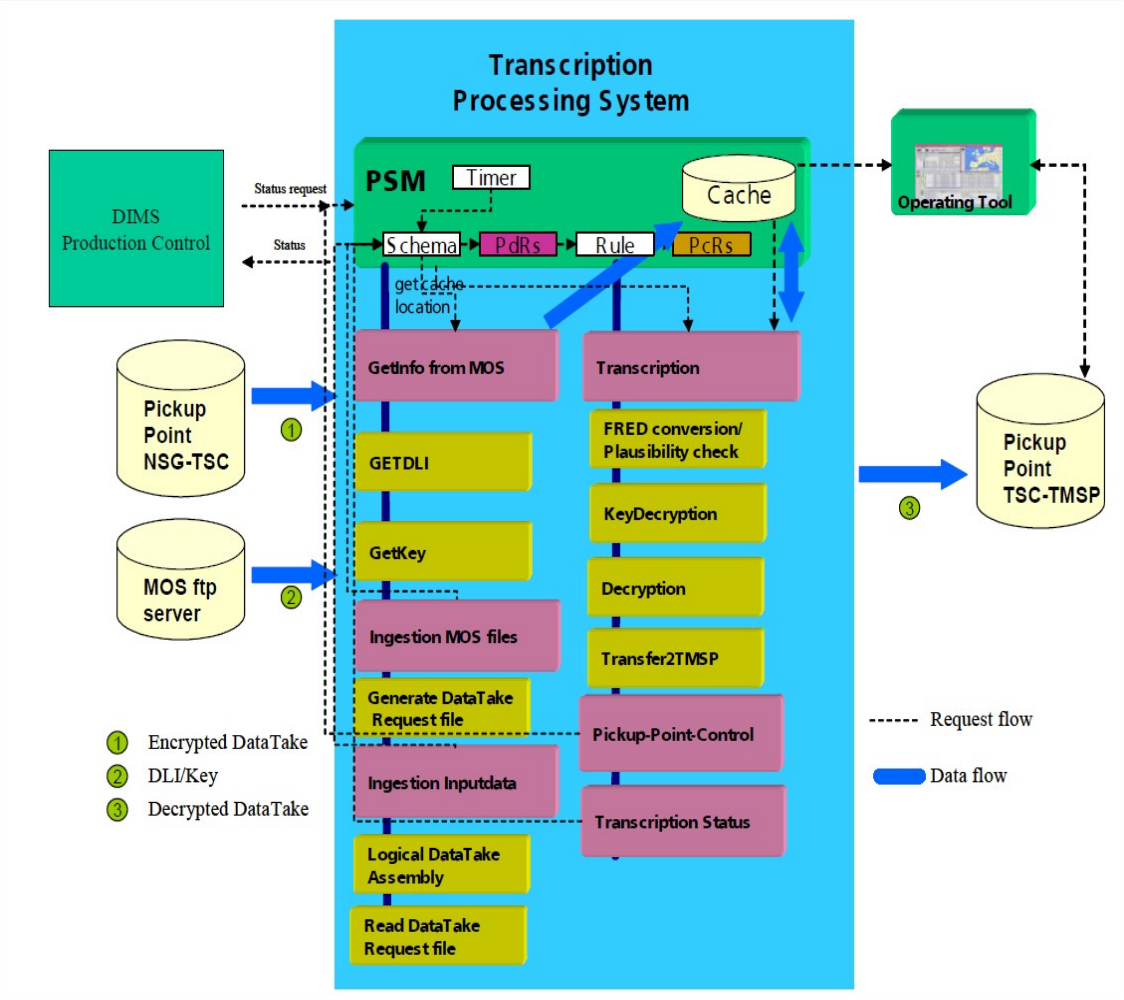

Abbildung 4-4 Komponenten und Umgebung des Transkription Prozessierungssystem der Bodenstation Neustrelitz [DLR03]

Im Umfang des EVG werden folgende Komponenten nicht betrachtet:

- DIMS Produktion Control
- Processing System Management (PSM)
- Operating Tool

Das Transkription Prozessierungssystem ist ein Subsystem des Nutzlastbodensegments und ist für die Entschlüsselung der Daten am Boden zuständig. Die Ver- und Entschlüsselung der Daten basiert auf einem kryptografischen Verfahren. Die Generierung und auch Bereitstellung der Schlüssel für die Ver- und Entschlüsselung wird von dem Team des Missionsbetriebssegments (MOS) übernommen und ist hier nicht Teil des Evaluierungsgegenstandes.

Für die Entschlüsselung der Daten wird ein Schlüssel verwendet, der auf einem definierten Übergabepunkt (Pickup Point) des Missionsbetriebssegments verschlüsselt

abgelegt wird. Die Verschlüsselung des Schlüssels ist ein asymmetrisches Verfahren. Das TSC erhält nun den verschlüsselten Schlüssel, entschlüsselt diesen Schlüssel mit seinem privaten Schlüssel und entschlüsselt die Daten mit diesem entschlüsselten Schlüssel. Das Public-Private-Key-Paar für die Verschlüsselung des Schlüssels wird in zeitlichen Abständen unter Verantwortung des TSC neu generiert. Der öffentliche Schlüssel für die Verschlüsselung des Schlüssels wird MOS zur Verfügung gestellt. Nach der Entschlüsselung soll der entschlüsselte Schlüssel sicher gelöscht werden, so dass er nicht wieder herstellbar ist. Um festzustellen, ob die empfangenen Radardaten ausreichende Qualität besitzen, werden die Radardaten für ein erstes systematisches Testverfahren (Screening) an der Bodenstation entschlüsselt.

Identifikation der Schutzziele

Für die Identifikation der Schutzziele wurde das Transkription Prozessierungssystem auf die TVRA-relevanten Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Abrechenbarkeit bzw. Nachweisbarkeit) untersucht. Die identifizierten Schutzziele wurden durch genaue Betrachtung des System und seiner Datenflüsse erhalten und sind im Annex A1 gelistet.

Identifikation der funktionalen Sicherheitsanforderungen

Dieser Schritt wurde analog wie bei der EVG Bodenstation durchgeführt. Für die funktionalen Sicherheitsanforderungen wurden die Klassen „Kryptographische Unterstützung“ und „Benutzerdatenschutz“ betrachtet. Die Ergebnisse befinden sich im Annex A1.

Systematische Bestandsaufnahme aller Assets (schützenswerte Güter)

Auch hier wurden die einzelnen Systembestandteile, vor allem in Bezug auf Telekommunikation, betrachtet und folgende schützenswerte Güter identifiziert und in die TVRA-Datenbank aufgenommen (vgl. Systematische Bestandsaufnahme aller Assets unter den EVG Bodenstation). Die relevanten schützenswerten Güter sind:

- Radardaten
- Schlüssel für die Entschlüsselung der Daten
- Privater Schlüssel
- Öffentlicher Schlüssel

Die Schritte:

- Systematische Identifikation der Verwundbarkeit
- Berechnung der Eintrittswahrscheinlichkeit eines Angriffes und seine Auswirkungen
- Beschreibung der Risiken
- Identifikation von Gegenmaßnahmen
- Kosten-Nutzen-Analyse der Gegenmaßnahmen

wurden vergleichbar zu den analogen Schritten bei der Anwendung der TVRA-Methode auf der Bodenstation durchgeführt. Die Ergebnisse befinden sich im Annex A1 und Annex A2 (*Risikoabschätzung* und *Gegenmaßnahmen-Kosten-Nutzen-Tabelle*).

Spezifikation von detaillierten Anforderungen

In diesem Schritt fließen gesonderte Anforderungen vom BSI für die Verschlüsselung und Entschlüsselung der Radardaten auf dem Boden ein. Für die Vertraulichkeit der Radardaten wird der TripleDES Algorithmus mit der Betriebsart Cipher Block Chaining (CBC) eingesetzt. Außerdem muss die X-Band- Kryptographische Funktion in der Lage sein, verschiedene Entschlüsselungseinheiten zu identifizieren.

Siehe Annex A1 für die entsprechenden detaillierten Anforderungen.

4.3 Webschnittstelle zur Suche, Bestellung und Auslieferung von Erdfernerkundungsdaten

Als Informationsgrundlage wurden das *TerraSAR-X Payload Ground Segment DIMS Configuration for TerraSAR-X* [DLR05], das *Data Information and Management System Design Document* [DLR06] und das *DIMS EOWEB Configuration Manual* [DLR07] verwendet.

Bestimmung des Evaluationsgegenstandes

Die Webschnittstelle soll Nutzer für die Suche, Bestellung und Auslieferung von Erdfernerkundungsdaten zur Verfügung gestellt werden.
Mit dieser Nutzerschnittstelle können Vorschaubilder angesehen werden, die bei der Auswahl der Erdfernerkundungsdaten unterstützen sollen.

Auch hier besteht der Evaluierungsgegenstand wiederum aus Hardware und Softwarekomponenten. Der Such-, Bestell- und Auslieferungsvorgang umfasst im Wesentlichen folgende Komponenten:

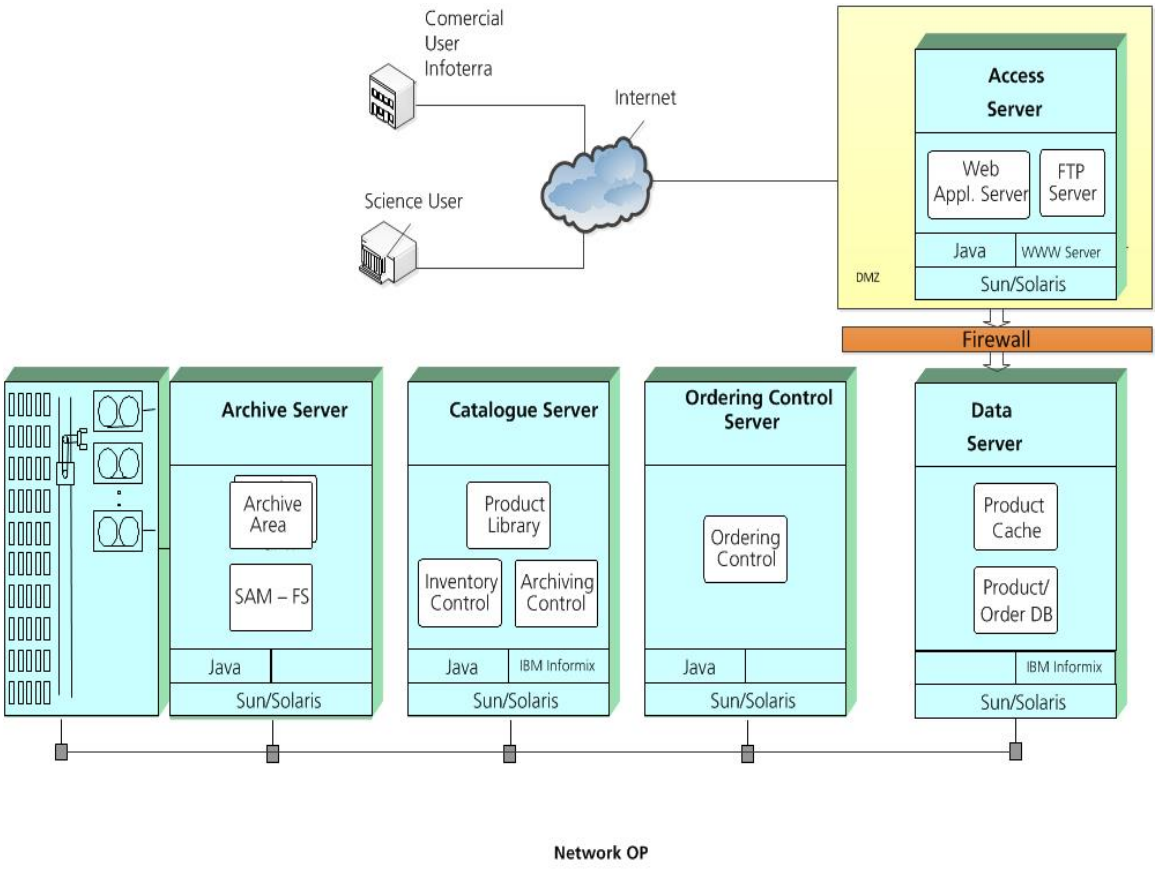

Abbildung 4-5 Komponenten der Webschnittstelle (Teile aus [DLR06])

Benutzerdaten, Radardaten, Vorschaubilder und Metadaten werden in einer sogenannten Produktbibliothek (Product Library) gespeichert. Weder Archivserver, Katalogserver, Datenserver noch Auftragskontrollserver sind Teil des Evaluierungsgegenstandes. Nur der Zugriffsserver ist Teil des Evaluierungsgegenstandes. Der Zugriffsserver besteht aus einem Webserver und einem FTP-Server.

Der Webservice ermöglicht die Registrierung und Autorisierung von Nutzern, da nicht allen Personen der Zugriff auf die Radardaten erlaubt ist. Die Daten dürfen nur an Personen ausgeliefert werden, die nicht in der EU-Sanktionsliste stehen. Neben dieser personenbezogenen Sanktionslistenprüfung werden auch personenunabhängige Länderembargos überwacht (vgl. [BJV07]).

Der Webserver stellt die Internetseiten für den Zugang der Erdfernerkundungsdaten über das Internet bereit. Die Informationen für die Webseiten werden in einer Datenbank innerhalb des DLR-Netzwerks abgelegt. Der Webserver sendet die Datenbankanfragen an den Katalogserver im geschützten LAN des DLR. Der Webserver hat Zugriff auf die Vorschaubilder und erlaubt, Bestellungen der Radardaten

auszuführen. Zusätzlich können Informationen über die verfügbaren Radardaten abgefragt werden.

Für die Auslieferung außerhalb des DLR werden zwei FTPS-Server in der DLR-D demilitarisierten Zone (DMZ) genutzt. Eine demilitarisierte Zone ist ein eigenständiges Subnetz, welches das lokale Netzwerk (LAN) durch Firewall-Router vom Internet trennt [EK16]. Gemäß dem FTPS-Protokoll erfolgt die Authentifizierung über Benutzername und Passwort, die Verschlüsselung der Übertragung über sitzungsbezogene Schlüssel.

Identifikation der Schutzziele

Für die Identifikation der Schutzziele wurde auch hier der EVG, in diesem Fall die Webschnittstelle, auf die TVRA-relevanten Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Abrechenbarkeit bzw. Nachweisbarkeit) untersucht. Die identifizierten Schutzziele wurden durch genaue Betrachtung des System und seiner Datenflüsse ermittelt. Die Ergebnisse befinden sich im Annex A1.

Identifikation der funktionalen Anforderungen

Dieser Schritt wurde analog wie bei dem EVG Bodenstation durchgeführt. Für die funktionalen Sicherheitsanforderungen wurden die Klassen „Kommunikation“, „Schutz der Benutzerdaten“ und „Identifikation und Authentifikation“ betrachtet. Die Ergebnisse befinden sich im Annex A1.

Systematische Bestandsaufnahme aller Assets (schützenswerte Güter)

Die schützenwerten Güter werden systematisch erfasst. Als schützenswerte Güter wurden

- Nutzerdaten
- Passwörter
- Ausgelieferte Produkte
- Webserver
- FTP-Server

identifiziert.

Für die systematische Erfassung dient die angelegte TVRA-Datenbank.

Bei dem betrachteten Evaluierungsgegenstand handelt es sich um eine Webanwendung. Aus diesem Grund wird für die Schritte:

- Systematische Identifikation der Verwundbarkeit
- Beschreiben der Risiken
- Identifikation von Gegenmaßnahmen

das Dokument „Die 10 häufigsten Sicherheitsrisiken für Webanwendungen“ [OWA13] des Open Web Application Security Project (OWASP) als Informationsgrundlage verwendet.

Die beiden Schritte

- Berechnung der Eintrittswahrscheinlichkeit eines Angriffes und seine Auswirkungen
- Kosten-Nutzen-Analyse der Gegenmaßnahmen

werden wiederum mit der Unterstützung durch und Befragung von Mitarbeitern durchgeführt.

Spezifikation von detaillierten Anforderungen

Unter Berücksichtigung von [DLR07] wurden folgende detaillierte Anforderungen spezifiziert:

- Die Verwendung der DLR Web- und FTP-Hosts für Angreifer, um in das DLR interne Netz zu gelangen, soll verhindert werden.
- Die Verwendung der DLR-Webschnittstelle für Angreifer, um in das DLR interne Netzt zu gelangen, soll verhindert werden.

Die gesammelten Ergebnisse sind in Annex A1 bzw. Annex A2 zu finden.

5 Untersuchung der Methode anhand eines hochwertigen Erdfernerkundungssystems

Die Methode sollte in den normalen Ablauf des Systems Engineering Prozesses eingebaut werden und während der einzelnen Phasen des Projektes wiederholt angewendet werden. Sobald die initialen Anforderungen spezifiziert werden, sollte die Analyse zum ersten Mal durchgeführt werden. Durch diese iterative Anwendung wird eine möglichst komplette Liste der Schutzziele und Anforderungen aufgestellt und die möglichen Risiken identifiziert.

Es müssen jederzeit neue Aspekte, die für den Evaluierungsgegenstand relevant werden, in die Methode eingebracht werden. Werden diese Informationen erst später erkannt, ist dies nicht so gravierend, da sie in der nächsten Iteration berücksichtigt werden. Die identifizierten Bedrohungen existieren weiterhin, jedoch können die Risiken eines Angriffes durch vorgenommene Sicherheitsmaßnahmen abgeschwächt werden.

5.1 Ergebnisse der Risikoanalyse

Die Anwendung der Methode liefert aufgrund der funktionalen Beschreibung des Systems die Bedrohungen und Schwachstellen, die das System besitzt. Anhand dieser Schwachstellen werden die Risiken sowie ihre möglichen Gegenmaßnahmen ermittelt. Ein Ergebnis der TVRA sind eine Reihe von Sicherheitsanforderungen, die notwendig sind, um das Risiko zu minimieren. Diese Gegenmaßnahmen resultieren in konkreten technischen Anforderungen an das System.

Mit der TVRA wird festgestellt, wie offen ein System gegenüber Angriffen ist, wobei die Schwachstellenanalyse hervorgehoben wird. Das Ergebnis einer Schwachstellenanalyse ist eine Liste von potenziellen Schwachstellen inklusiv der Information, wie leicht diese Schwachstellen für einen Angriff ausgenützt werden können. Bei der TVRA wird viel Wert auf die Gegenmaßnahmen und ggf. eine Neugestaltung des Systems gelegt. Es ist hierbei zu beachten, dass die Gegenmaßnahmen selbst auch ihre eigenen Schwachstellen haben und zu Assets, also zu schützenswerten Gütern des Systems, werden können.

Bei der Durchführung der Methoden wurden insgesamt 15 Risiken erkannt, von denen sieben als kritisch, sechs als bedeutend und zwei als gering eingestuft wurden:

- Stören des Datenempfangs (kritisch)
- Man-in-the-Middle Angriff zwischen der Antenne und der Empfangsausrüstung (kritisch)
- Cross-Site Request Forgery (Angreifer generiert eine gefälschte HTTP-Anfrage) (kritisch)
- Nutzen von Software mit bekannten Schwachstellen (kritisch)
- Nutzen von Anwendungen mit Weiterleitung (kritisch)
- Session-Hijacking (kritisch)
- Syn-Flood (kritisch)
- Portscan (bedeutend)
- Erraten oder systematisches Ausprobieren des Passwortes (bedeutend)
- Identitätsdiebstahl (bedeutend)
- Man-in-the-Middle Angriff zwischen FTP-Server und Rechner eines legalen Benutzers (bedeutend)
- Abhören der Radardaten durch Datenempfang an einer unautorisierten Antenne (bedeutend)
- Anzapfen der Kommunikationsverbindung zwischen der Antenne und der Empfangsausrüstung (bedeutend)
- Anzapfen der Kommunikationsverbindung zwischen MOS-FTP-Server und TSC (gering)
- Man-in-the-Middle Angriff zwischen MOS-FTP-Server und TSC (gering)

Der Einsatz der identifizierten Gegenmaßnahmen wurde zum größten Teil als positiv oder ohne Bedeutung bewertet. Die Gegenmaßnahmen können im Annex A2 eingesehen werden.

Die Ergebnisse hängen stark von den Kenntnissen über die funktionalen Zusammenhänge der Prozesse und der internen Abläufe des Erdfernerkundungssystems sowie der Personen, die die Methode ausführen und deren Erfahrungen und subjektiven Bewertungen ab.

Im Rahmen des Auftragsabwicklungsprozesses fordert das SatDSiG, dass bestimmte Daten aufgezeichnet und mindestens fünf Jahre lang aufbewahrt werden müssen. Hierunter fallen die Langzeitarchievierung der Auftragsdaten und der Nachweis der benötigten Log Files.

Das betrachtete Erdfernerkundungssystem wurde vor dem Inkrafttreten des Gesetzes entwickelt und konstruiert. Aus diesem Grund fehlen sämtliche Schnittstellen bei den Teilkomponenten für die systematische Archivierung und das Extrahieren der Daten. Das Fehlen dieser Sicherheitsanforderung wurde bei der Durchführung der Analyse mit der TVRA-Methode nicht erkannt, da das Schutzziel Revisionsfähigkeit (Reviewability) unbeachtet bleibt.

5.2 Bewertung der Methode auf der Basis von Bewertungskriterien

Die TVRA-Methode war nicht immer einfach zu befolgen, sie war jedoch dennoch nützlich in dieser Analyse. Insgesamt ist die Methode sehr gut beschrieben, einige Verbesserungen wären jedoch für die praktische Umsetzung vorteilhaft. Für die Generierung von hochwertigen und genauen Ergebnissen ist es wichtig den Evaluierungsgegenstand sehr genau zu beschreiben. In der Spezifikation der TVRA-Methode wird die Vorgehensweise für den Schritt „Bestimmung des Evaluierungsgegenstandes“ nicht genau beschrieben. Außerdem benötigt sie eine einfache Vorgehensweise, um die Identifikation der Bedrohungen und Verwundbarkeiten zu erleichtern [Mo09].

In dem Schritt der Kosten-Nutzen-Analyse der Gegenmaßnahmen soll eine Entscheidung für oder gegen die Sicherheitsmaßnahme ermöglicht werden und diese Entscheidung soll zudem überprüfbar sein. Jedoch ist dieser Schritt nicht einfach umsetzbar, da die Erfassung von Kosten einer Sicherheitsmaßnahme oder die Quantifizierung ihres Nutzens nur schwer durchgeführt werden können. Für den praktischen Einsatz werden leicht verständliche Herangehensweisen benötigt (vgl. [No05]).

Um Herauszufinden, wie gut die Methode für eine Risikoanalyse angewendet werden kann, wurde eine Reihe von Fragen bezüglich verschiedener Kriterien aufgestellt. Die Kriterien wurden angelehnt an die Veröffentlichung von [Ki13].

Kriterien	**Antworten**
Ist die Methode wirklich eine Methode oder ein Standard oder eine Richtlinie?	Die TVRA ist ein Standard und eine Methode.
Identifiziert die Methode	Ja, die Methode identifiziert

Informationssicherheitsrisiken?	Informationssicherheitsrisiken.
Gibt es eine Dokumentation zu der Methode und wie teuer ist diese?	Ja, die Methode ist sehr systematisch dokumentiert, jedoch sind nicht alle notwendigen Tabellen der Datenbank erwähnt oder vollständig beschrieben. Dies kann ggf. vernachlässigt werden, da die Nutzung einer Datenbank zur Unterstützung der Anwendung der Methode optional ist. Die Dokumentation ist kostenlos erhältlich.
Wann wurde die Methode zuletzt überarbeitet?	Die letzte Veröffentlichung der TVRA-Methode stammt aus dem Jahr 2011.
Ist zusätzliche Software notwendig und entstehen dadurch weitere Kosten?	Zur Unterstützung der Anwendung der Methode wird eine Datenbank angeraten. Der Nutzen der Anwendung der Methode mit Hilfe der Datenbank ist sehr hoch, da die benötigten Informationen, die in der Datenbank gespeichert sind, der TVRA bereitgestellt werden können und somit die Verwaltung der Daten vereinfacht wird. Diese Datenbank wird als interaktives Tool der TVRA Methode betrachtet. In dieser Arbeit wurde eine MySQL Datenbank verwendet. Die Nutzung der Datenbank verursacht keine Kosten, bis auf den zeitlichen Aufwand für die Erstellung und dem Füllen der Datenbank mit Informationen, sowie dem benötigten Festplattenplatz für die Daten und die Datenbank selber.
Welche Voraussetzungen und welches Fachwissen muss der Anwender der Methode mitbringen?	Der Anwender sollte Detailwissen über das zu untersuchende System besitzen und sich sehr gut mit IT-Risikoanalysen auskennen. Positiv für die Anwendung dieser Methode sind Kenntnisse über Datenbanken, die das strukturierte und

	systematische Erfassen der Daten sowie die Berechnung der Risiken erleichtert.

Wie im Kapitel 5.5 näher erläutert wird, kann die Methode für die Anwendung der Risikoanalyse an das Szenario Erdfernerkundungssystem angepasst werden.

5.3 Vergleich der TVRA mit der Risikoanalyse nach IT-Grundschutz

Der Vergleich wird in Bezug auf benötigte Zeit, Anzahl der vorgeschlagenen Sicherheitsmaßnahmen und der Anzahl der unterschiedlichen Bedrohungskategorien durchgeführt.

Beide Risikoanalysemethoden sind qualitative Risikoanalysemethoden. Bei der Mission TanDEM-X wurde die Risikoanalyse nach IT-Grundschutz von externen Sicherheitsexperten durchgeführt. Das System und die einzelnen Systemelemente wurden in einem sehr niedrigen Detaillierungsgrad betrachtet. Diese Betrachtungsweise kann hier nur bedingt zum Vergleich verwendet werden. Die Ergebnisse der Risikoanalyse wurden innerhalb des Sicherheitskonzeptes [DLR09] gemäß SatDSiG für die Missionen TerraSAR-X und TanDEM-X beschrieben. Dieses Dokument darf aufgrund der Sicherheitsanforderungen an das Projekt nicht an diese Arbeit angehängt oder anderweitig veröffentlicht werden. Nachfolgend werden Auszüge des Dokuments genannt, die für diese Arbeit relevant sind.

Bei der Risikoanalyse auf der Basis des IT-Grundschutzes werden zunächst Maßnahmen für die Sicherheit gesichtet und dann untersucht, welche Maßnahmen mit einem vertretbaren Aufwand umgesetzt werden sollen. Diese Vorgehensweise benötigt Kenntnisse über die IT-Sicherheit und die Informationsverarbeitung. Im Gegensatz zur TVRA-Risikoanalyse benötigt sie aber keine Kenntnisse über eine bestimmte Methode. Dadurch ist der Aufwand geringer und somit kostengünstiger und schneller umsetzbar. Bei der TVRA-Risikoanalyse wird das konkrete Gefährdungspotential im Detail untersucht. Eine Kosten-Nutzen-Analyse der Gegenmaßnahmen wurde bei der Risikoanalyse nach IT-Grundschutz nicht durchgeführt. Die TVRA-Analyse ist umfangreicher, hat einen höheren Aufwand und es wird mehr Zeit für die Durchführung benötigt.

Gemäß dem IT-Grundschutz wird untersucht, welche Schäden beim Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Die Klassifizierung von Schäden wird durch die Schutzbedarfskategorien beschrieben. Im Rahmen des IT-Grundschutzes werden drei Schutzbedarfskategorien definiert:

- "normaler Schutzbedarf": Die Schadensauswirkungen sind begrenzt und überschaubar.
- "hoher Schutzbedarf": Die Schadensauswirkungen können beträchtlich sein.
- "sehr hoher Schutzbedarf": Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

[BSI01]

Auf Grund der Anforderungen des SatDSiG wurden bei der Risikoanalyse nach IT-Grundschutz im TanDEM-X Projekt folgende Schutzbedarfe erkannt:

- Die Kommandierungsfolgen haben einen hohen Schutzbedarf hinsichtlich *Integrität* der Daten.
- Die Radardaten haben einen hohen Schutzbedarf hinsichtlich der *Vertraulichkeit* der Daten.

Auszug aus [DLR09].
Weitere Schutzbedarfe sind im SatDSiG nicht genannt und bei der Risikoanalyse innerhalb der TanDEM-X Mission nicht betrachtet worden.

Allen erkannten Risiken wird mit organisatorischen oder technischen Maßnahmen begegnet, um die Risiken in einem akzeptablen Maß zu halten.
Die Überwindung der Sicherheitsmaßnahmen erfordert sowohl erhebliche Fachkenntnisse als auch die Mitarbeit eines fachkundigen Innentäters.

Als organisatorische Maßnahmen sind solche Schutzversuche zu verstehen, die durch Handlungsanweisung bzw. Verfahrens- und Vorgehensweisen umgesetzt werden. Beispiele hierfür sind

- Besucheranmeldung
- Vier-Augen-Prinzip
- Festgelegte Intervalle zur Stichprobenprüfungen

(vgl. [BFD16])

Die Anzahl der Sicherheitsmaßnahmen bei der Risikoanalysemethode auf der Basis des IT-Grundschutzes liegt gemäß [DLR09] bei acht:

- Erhöhter Zugangsschutz
- Einsatz überprüfter Mitarbeiter
- Gesicherte Aufstellung
- Absicherung des Netzsegments
- Abschalten nicht benötigter Dienste
- Erhöhter Zugangsschutz zu Netzkomponenten
- Erhöhter Schutz des Netzzugangs in der Firewall
- Aufteilung der DMZ in ein öffentliches und ein internes Segment

Bei der TVRA wird das System auf die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Abrechenbarkeit hin untersucht.

Es wurden hierbei die gleichen drei Schutzbedarfskategorien, wie bei der Risikoanalyse nach BSI-Grundschutz zu Grunde gelegt und folgende Schutzbedarfe erkannt:

- Die Bodenstation hat einen hohen Schutzbedarf hinsichtlich der Verfügbarkeit der Empfangsanlage.
- Die Radardaten haben einen hohen Schutzbedarf hinsichtlich der Integrität der Daten.
- Die Radardaten haben einen hohen Schutzbedarf hinsichtlich der Vertraulichkeit der Daten.
- Zugangsdaten des Webservices für die Bestellung der Daten haben einen hohen Schutzbedarf der Authentizität.
- Der Webserver hat einen hohen Schutzbedarf hinsichtlich der Verfügbarkeit.
- Der FTP-Server hat einen hohen Schutzbedarf hinsichtlich der Verfügbarkeit.

Jedoch werden bei der TVRA nur technische Gegenmaßnahmen betrachtet, um die Risiken in einem akzeptablen Maß zu halten. Auch hier erfordert die Überwindung der Sicherheitsmaßnahmen, sowohl erhebliche Fachkenntnisse als auch die Mitarbeit eines fachkundigen Innentäters.
Bei der TVRA-Methode wurden 15 Sicherheitsmaßnahmen erkannt:

- Einzäunen der Antenne und der Empfangsanlage
- Nur autorisierte Personen haben Zugang zu dem Gelände, auf dem sich die Antenne befindet

- Nur autorisierte Personen haben Zugang zu den Räumen der Empfangsanlage
- Bei der FTP-Übertragung ein gemeinsames Datenverschlüsselungssystem nutzen
- Schließen von nicht benutzen Ports
- Überwachen typischer Kennwerte, wie Netzwerk- oder Speicherauslastung
- Benutzen eines zentralen Mechanismus für die Authentifizierung
- Benutzen der aktuellsten Version der verwendeten Software
- Anwenden von starken Passwortrichtlinien
- Einsatz einer Firewall
- Jede Webseite sollte einen einzigartigen Token besitzen
- Setzen des httponly-Flags, um das Lesen und Manipulieren der Daten zu verhindern
- Nicht überprüftes Weiterleiten deaktivieren
- Verwenden von indirekten Objektreferenzen
- Zuweisung minimaler Rechte an Nutzer

Das Verfahren wird bei der TVRA iterativ angewendet, bis das Risiko auf ein akzeptables Niveau reduziert wird, oder wenn sich Änderungen im Einsatzgebiet ergeben, die ein erneutes Durchlaufen der TVRA erfordern.
Der Detailierungsgrad der TVRA hängt demnach von der Anzahl der Iterationen, die die TVRA-Methode durchlaufen hat, ab.

5.4 Diskussion der Ergebnisse

Der Verlust des Satelliten durch fehlerhafte Kommandierung oder Kommunikationsverlust erzeugt einen Schaden in Höhe von mehreren Hundert Millionen Euro. Dieser Schaden ist (soweit möglich) durch eine Versicherung zu decken, die in der Prämienberechnung von den oben genannten Maßnahmen ausgeht. Die mögliche Schadenshöhe ist in der Bewertung des Schutzbedarfs "sehr hoch" hinsichtlich der Verfügbarkeit der Kommandierungsstrecke berücksichtigt.

Weiterhin wurde festgestellt, dass eine detaillierte Bewertung der in der Risikoanalyse erkannten Risiken hinsichtlich der möglichen Schadenshöhe aus folgendem Grund nicht praktikabel sei:

Der wirtschaftliche Wert der SAR-Aufnahmen ist nicht bezifferbar. Er ist auf jeden Fall erheblich höher als der nominelle Preis, der von wissenschaftlichen Nutzern für die Lizenzierung zu zahlen ist.
Diese Situation ist der Projektleitung und dem Missionsmanagement bewusst, die daraus resultierenden Unsicherheiten werden akzeptiert. Aus diesem Grund wurde dieser Aspekt bei beiden Risikoanalysen nicht betrachtet.

Die TVRA bezieht relevante Teile der Common Criteria ein und hat zum Ziel, hochwertige Ergebnisse zu liefern, die als Eingabe für eine Bewertung der Sicherheit gemäß den Common Criteria dienen. Bei der Analyse nach IT-Grundschutz wurde vom BSI ein Zertifizierungsschema für Informationssicherheit entwickelt. Hierbei werden für die Informationssicherheit Anforderungen aus ISO/IEC 27001 berücksichtigt [BSI02]. Die Ergebnisse sollten demnach vergleichbar sein, dennoch beruhen die unterschiedlichen Ergebnisse unter anderem auf der Tatsache, dass unterschiedliche Personen die Analysen durchgeführt haben. Diese Personen besitzen unterschiedliche Fachkenntnisse über das System, über Informationssicherheit, und können auf unterschiedliche Erfahrungsschätze zugreifen. Eine Erklärung, warum die TVRA-Methode mehr Sicherheitsmaßnahmen als die Risikoanalyse nach IT-Grundschutz erkannt hat, liegt darin, dass die TVRA-Methode das System detaillierter betrachtet.

Positiv bei der Anwendung einer Risikoanalyse ist schon allein die Tatsache, dass die Personen gezwungen sind, sich mit dem System auseinander zusetzten. Dadurch erhalten sie einen besseren Zugang zum System. Außerdem werden sicherheitskritische Aspekte erkannt, die näher betrachtet werden sollen.

5.5 Anpassungen der Methode für die Anwendung an ein hochwertiges Erdfernerkundungssystem

Die Verwendung der TVRA ist auf folgende fünf Bedrohungskategorien ausgerichtet:

- Abhören von Daten (Interception)
- Unbefugtes Ändern von Daten (Manipulation)
- Verhindern/Unterbrechen der Kommunikationsbeziehung (Denial of Service)
- Verleugnung der Teilnahme an einer Kommunikation (Repudiation) durch den Sender

- Verleugnung der Teilnahme an einer Kommunikation (Repudiation) durch den Empfänger

Bei der Aufstellung der Schutzziele sind folglich nur diese Bedrohungskategorien betrachtet worden. Jedoch schließt die Anwendung der TVRA weitere Bedrohungskategorien nicht aus, so dass die Methode für die Anwendung an ein hochwertiges Erdfernerkundungssystem angepasst werden kann, indem weitere Bedrohungskategorien hinzugefügt werden. Zu den ursprünglichen fünf Kategorien sollten die Kategorien Verschleierung der eigenen Identität, Phishing und Erhöhung von Berechtigungen hinzugefügt werden. Ein immer stärker werdender Faktor im Bereich der Informationssicherheit ist das Social Engineering. Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z.B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln [BSI08]. Dieser Faktor sollte nicht unbeachtet bleiben. In der Veröffentlichung [Ra13] wird darauf hingewiesen, dass der Faktor Mensch bei Informationssicherheit bisher nicht einbezogen wird. Es existieren dennoch einige Überlegungen, darüber, wie Menschen die Informationssicherheit beeinträchtigen, indem sie Sicherheitslücken hervorrufen oder indem sie risikobehaftete Entscheidungen treffen.

Wie in Unterkapitel 5.1 bemerkt, wird das Schutzziel Revisionsfähigkeit bei der Analyse nicht betrachtet. Es existieren diesbezüglich keine funktionalen Sicherheitsanforderungen an das System. Dies hat zur Folge, dass sämtliche Schnittstellen bei den Teilkomponenten für die systematische Archivierung und das Extrahieren der Daten unbemerkt fehlen. Um das Fehlen dieser Schnittstellen zu erkennen, sollten, zusätzlich zu den betrachteten fünf Arten der Schutzziele Vertraulichkeit (Confidentiality) , Integrität (Integrity), Verfügbarkeit (Availability), Abrechenbarkeit (Accountability) und Authentizität/Nachweisbarkeit (Authenticity), weitere Schutzziele, wie z. B. die Revisionsfähigkeit, betrachtet werden.

Wünschenswert wären detaillierte Vorgaben für die Durchführung der Kosten-Nutzen-Analyse. Dadurch würde der stark subjektive Charakter der Analyse reduziert werden. Weitere Anpassungen sind nicht betrachtet worden.

6 Zusammenfassung

Die vorliegende Arbeit bietet zunächst eine Einführung in das Thema Anwendung und Untersuchung einer Methode zur Analyse von IT-Sicherheitsrisiken anhand eines hochwertigen Erdfernerkundungssystems. Den Hauptteil bildet die Beschreibung der Threat, Vulnerability and Risk Analysis-Methode und der Erkenntnisse ihres praktischen Einsatzes anhand eines hochwertigen Erdfernerkundungssystems.

Der Erfolg dieses Verfahrens hängt sehr stark vom Fachwissen der Spezialisten für IT-Risiken ab, wobei diese Eigenschaft bei allen analysierten Risikoanalysemethoden der Fall ist. Durch die strukturierte Dokumentation ist die Methode benutzerfreundlich. Jedoch ist sie auch sehr komplex, so dass dies einige Benutzer vor der Verwendung der Methode abschrecken könnte. Der Schritt Systematische Identifikation der Verwundbarkeit ist in zu viele Unterschritte gegliedert. An dieser Stelle könnte die Methode verkürzt werden und die Schritte Identifikation der Schwachstellen und Identifikation der Verwundbarkeit zusammengefasst werden. Die Methode ist transparent und vollständig, da es keine sogenannten Blackboxes gibt, sondern die Anwendung an allen Stellen nachvollziehbar ist. Dies vermittelt Vertrauen und Verständnis für die Methode. Dies ist auch aus Gründen der Standardisierung und Anwenderakzeptanz wichtig.

Korrelationen zwischen den Risiken sind innerhalb der Methode nicht berücksichtigt. Die einzige Beziehung zwischen den Risiken kann dadurch entstehen, dass Gegenmaßnahmen wiederum selber zu schützenswerten Gütern werden.

Die zeitlichen Veränderungen von Risiken werden in der Methode betrachtet, da die Methode als ein iterativer Prozess angesehen wird. Wie oft und in welchen zeitlichen Abständen die Methode erneut durchgeführt wird, hängt von dem Anwender der Methode ab. Die Zeitintervalle sind nicht fest vorgegeben. Dadurch, dass die TVRA zyklischer Natur ist und bei der Herstellung des Systems immer weiter verfeinert wird, deckt die Methode fast den gesamten Lebenszyklus des Projektes ab. Anforderungsanalyse, Entwurf (Identifikation der Sicherheitsanforderungen), Verifikation und Validierung sowie auch Betrieb (Sicherheitsbestimmungen) finden sich in dieser Methode wieder. Die Konzeptphase und die Entsorgung werden dagegen nicht abgedeckt.

Eine Risikoanalyse ist häufig sehr aufwendig. Die TVRA geht davon aus, dass die Risikoanalyse iterativ durchlaufen wird. Dies führt dazu, dass die Schritte öfters durchlaufen werden, die Gegenmaßnahmen hierdurch aber auch früher umgesetzt werden. Es ist schwierig, zu entscheiden, wann die TVRA genügend oft durchlaufen wurde. Dies ist eine Abwägung von Zeit, Kosten und IT-Sicherheit des gesamten Systems.

Die getroffenen Schutzmaßnahmen werden nur insofern überprüft, als ein neuer Iterationsschritt der TVRA-Methode durchlaufen wird. Hierbei wird das System wieder systematisch nach bestehenden Schwachstellen durchsucht.

Da die Methode einer TVRA-Analyse einem festen Schema folgt, besteht die Gefahr, dass es weniger flexibel als andere Risikoanalysemethoden ist.

Risikoanalysemethoden sind ein wichtiger Teil für das Design, die Entwicklung und die Herstellung von IT-Systemen. Die TVRA-Methode stellt einen kompletten Ansatz zur Risikobewertung dar, bietet aber noch Raum für Verbesserungen. Die Methode bietet eine umfassende Möglichkeit an, um die Sicherheitsrisiken, die bekämpft werden müssen, zu identifizieren. Aber diese Methode liefert nicht automatisch die notwendigen Sicherheitsmaßnahmen. Es wird Fachwissen und eine manuelle Auswahl benötigt, um diese Aufgabe zu erfüllen.

Zukünftig wäre es sinnvoll die Methode zu erweitern, da sie lediglich auf Kommunikationssysteme spezialisiert ist. Es könnten schon im Vorfeld weitere Bedrohungskategorien wie zum Beispiel Verschleierung der eigenen Identität oder Social Engineering in die Methode einfließen, um sie für ein breiteres Anwendungsgebiet verwenden zu können. Des Weiteren sollte der Benutzer des Systems und sein Fehlverhalten in dieser Methode berücksichtigt werden. In der Praxis sind oft personelle und organisatorische Sicherheitsmaßnahmen zu treffen, um die Sicherheit eines IT-Systems zu gewährleisten. Identitätsdiebstahl und Rechteausweitung sind Angriffspunkte bei komplexen Angriffen. Diese Aspekte werden bei der TVRA-Analyse kaum in Betracht gezogen, denn sie konzentriert sich insbesondere auf sichere IT-Komponenten.

Es ist abzuwägen, ob der benötigte zeitliche Aufwand für die Erstellung der TVRA-Risikoanalyse für das Anwendungsszenario gerechtfertigt ist, wenn keine Zertifizierung des Systems angestrebt wird.

7 Quellenverzeichnis

[AD03] Christopher Alberts, Audrey Dorofee: *Managing Information Security Risks: The Octave Approach*, Pearson Education Inc., 2003.

[An01] Ross Anderson: *Why Information Security is Hard - An Economic Perspective.* Proceedings of 17th Annual Computer Security Applications Conference (ACSAC), S. 10–14, 2001.

[An08] Ross Anderson: *Security Engineering. A Guide to Building Dependable Distributed Systems*. 2.Auflage, Wiley, 2008, ISBN 978-0-470-06852-6.

[Ba01] Kurt G. Baldenhofer: *Lexikon der Fernerkundung*, http://www.fe-lexikon.info/FeLexikon.htm, letzter Zugriff 21.07.15.

[Ba98] Helmut Balzert: *Lehrbuch der Software- Technik: Software-Management, Software-Qualitätssicherung, Unternehmensmodellierung, Spektrum* Akademischer Verlag, 1998, ISBN 3827400651.

[BA10] Mark Bedner, Tobias Ackermann: *Schutzziele der IT-Sicherheit*, Datenschutz und Datensicherheit, 5, S. 323-328, 2010.

[BD07] BITKOM, DIN: *Kompass der IT-Sicherheitsstandards Leitfaden und Nachschlagewerk* , 2007.

[BFD16] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Technische und organisatorische Maßnahmen gemäß Bundesdatenschutzgesetz (BDSG)*, https://www.bfdi.bund.de/bfdi_wiki/index.php/Technische_und_organisatorische_Maßnahmen, letzter Zugriff 25.03.2016.

[BJV07] Bundesministerium der Justiz und für Verbraucherschutz, *Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz – SatDSiG)*, 2007.

[BJV08] Bundesministerium der Justiz und für Verbraucherschutz, *Verordnung zum Satellitendatensicherheitsgesetz (Satellitendatensicherheitsverordnung – SatDSiV)*, 2008.

[BL04] W. G. Bornman, L. Labuschagne: *A comparative framework for evaluating information security risk management methods*, Proceedings of the Information Security South Africa Conference, 2004.

[BMW08] Bundesministerium für Wirtschaft und Energie (BMWi): *Hintergrundinformation zum Satellitendatensicherheitsgesetzes SatDSiG und zur Rechtsverordnung SatDSiV*, 2008.

[BNA15] Bundesnetzagentur, *ETSI*, http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Technik/Standardisierung/InternVerbdgUndKoordinierungsstelle/ETSI/etsi-node.html, letzte Zugriff 07.10.2015.

[Bo15] Aymen Boudguiga et al.: *RACE: Risk analysis for cooperative engines*, 7th International Conference on New Technologies, Mobility and Security (NTMS), S.1-5, 2015.

[BRC12] Armaghan Behnia, Rafhana Abd Rashid, Junaid Ahsenali Chaudhry: *A Survey of Information Security Risk Analysis Methods*, Smart Computing Review, vol. 2, no. 1, S. 79-94, 2012.

[BRD07] Bundesregierung, *Entwurf eines Gesetzes zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz – SatDSiG)*, 2007.

[BSI01] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)*, 2008.

[BSI02] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI Standard 100-2: IT-Grundschutz-Vorgehensweise*, 2008.

[BSI03] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz*, 2008.

[BSI04] Bundesamt für Sicherheit in der Informationstechnik (BSI): *4 Glossar und Begriffsdefinitionen*, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/glossar/04.html letzte Zugriff 11.12.2015.

[BSI05] Bundesamt für Sicherheit in der Informationstechnik (BSI): *1.3 IT-Grundschutz und Informationssicherheit*, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursITGrundschutz/WarumITGrundschutz/itgrundschutzundis/itgrundschutzundis_node.html, letzter Zugriff 11.12.15.

[BSI06] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik*, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/CommonCriteria/commoncriteria_node.html, letzter Zugriff 11.12.15.

[BSI07] Bundesamt für Sicherheit in der Informationstechnik (BSI): *BSI TR-03140 Conformity assessment according to the satellite data security act (TR-SatDSiG)*, 2013.

[BSI08] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Kataloge*, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, letzter Zugriff 28.03.16.

[CC01] Common Criteria for Information Technology Security Evaluation *Part 1: Introduction and general model*, 2012.

[CC02] Common Criteria for Information Technology Security Evaluation *Part 2: Security functional components*, 2012.

[CC03] Common Criteria for Information Technology Security Evaluation *Part 3: Security assurance components*, 2012.

[CEM] Common Methodology for Information Technology Security Evaluation, *Evaluation methodology*, 2012.

[Ci97] Zbigniew Ciechanowicz: *Risk Analysis: requierements, conflicts and problems*, Computer & Security, Vol. 16, No. 3, S.223-332, 1997.

[Ci15] Cisco: *Cisco 2015 Annual Security Report*; 2014.

[Di04] Rüdiger Dierstein: *Sicherheit in der Informationstechnik—der Begriff IT-Sicherheit*, Informatik Spektrum, S. 343-353, 2004.

[DLR01] Deutsches Zentrum für Luft und Raumfahrt, *Synthetisches Apertur Radar (SAR)* , http://www.dlr.de/dlr/desktopdefault.aspx/tabid-10389/, letzter Zugriff 27.12.15.

[DLR02] Deutsches Zentrum für Luft und Raumfahrt, *TanDEM-X Ground Segment Ground Station Network Design Document (S-326)*, 2008, nur DLR intern.

[DLR03] Deutsches Zentrum für Luft und Raumfahrt, *Transcription System Design Document*, 2004, nur DLR intern.

[DLR04] Deutsches Zentrum für Luft und Raumfahrt, *TX-PGS-UM-2028_Transcription-System-User-Manual_1.0*, 2006, nur DLR intern.

[DLR05] Deutsches Zentrum für Luft und Raumfahrt, *TerraSAR-X Payload Ground Segment DIMS Configuration for TerraSAR-X*, 2015, nur DLR intern.

[DLR06] Deutsches Zentrum für Luft und Raumfahrt, *Data Information and Management System Design Document*, 2009, nur DLR intern.

[DLR07] Deutsches Zentrum für Luft und Raumfahrt, *DIMS EOWEB Configuration Manual*, 2015, nur DLR intern.

[DLR08] Deutsches Zentrum für Luft und Raumfahrt, *TanDEM-X / TerraSAR-X - Security Requirements and Data Policy Principles* -, 2010, nur DLR intern.

[DLR09] Deutsches Zentrum für Luft und Raumfahrt, *Sicherheitskonzept gemäß SatDSiG für die Missionen TerraSAR-X und TanDEM-X*, 2015, nur DLR intern.

[EK16] Elektronik-Kompendium, *DMZ – Demilitarisierte Zone*, http://www.elektronik-kompendium.de/sites/net/0907241.htm, letzter Zugriff 14.03.16.

[Ec14] Claudia Eckert: *IT-Sicherheit – Konzepte – Verfahren – Protokolle*, 9. Auflage, Oldenbourg Wissenschaftsverlag, 2014. ISBN: 978-3-486-85916-4.

[ET15] Marko Esche, Florian Thiel: *Software risk assessment for measuring instruments in legal metrology*, Proceedings of the Federated Conference on Computer Science and Information Systems, S. 1113–1123, 2015.

[ETS16] Europäisches Institut für Telekommunikationsnormen (ETSI), *Intelligent Transport Systems*, www.etsi.org/technologies-clusters/technologies/intelligent-transport, letzter Zugriff 12.01.16.

[ETS11] Europäisches Institut für Telekommunikationsnormen (ETSI): *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis (ETSI TS 102 165-1 V4.2.3)*, 2011.

[ETS10] Europäisches Institut für Telekommunikationsnormen (ETSI): *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA) (ETSI TR 102 893 V1.1.1)*, 2010.

[ETS08] Europäisches Institut für Telekommunikationsnormen (ETSI): *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards -guide, method and application with examples (ETSI TR 187 011 V2.1.1)*, 2008.

[Fr14] Felix Freiling et al.: *Technische Sicherheit und Informationssicherheit Unterschiede und Gemeinsamkeiten*, Informatik-Spektrum, Volume 37, Issue 1, S. 14-24, 2014, Print ISSN: 0170-6012.

[Ha01] Haufe Gruppe: *Dateien und Datenträger sicher löschen / 3 Standards und Verfahren zum sicheren Löschen*, http://www.haufe.de/unternehmensfuehrung/profirma-professional/dateien-und-datentraeger-sicher-loeschen-3-standards-und-verfahren-zum-sicheren-loeschen_idesk_PI11444_HI2288085.html, letzter Zugriff 12.10.15

[ISO11] ISO/IEC 27005:2011: (E): *Information technology — Security techniques —Information security risk management*, International Standard, 2011

[ISO14] ISO/IEC 27000:2014 (E): *Information technology — Security techniques —Information security management systems* — Overview and vocabulary, 2014.

[Ki13] Kiran K.V.D. et al.: *Performance And Analysis Of Risk Assessment Methodologies In Information Security*, International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 10, S. 3685 - 3692, 2013.

[KOJ12] Kleberger P., Olovsson T, Jonsson E.: *An In-Depth Analysis of the Security of the Connected Repair Shop*, The Seventh International Conference on Systems and Networks Communications (ICSNC), S. 99 - 107, 2012.

[Kö13] Hans-Peter Königs: *IT-Risikomanagement mit System*, 4.Aufl.,Springer, 2013, ISBN 978-3-8348-1687-0.

[Kr03] Helmut Krcmar: *Informationsmanagement*, 3. Aufl ., Springer, 2003 ISBN 978-3-540-43886-1.

[KS05] Bilge Karabacaka, Ibrahim Sogukpinar: *ISRAM: information security risk analysis method*, Computer and Security, S. 147-159, 2005.

[Le14] Ming-Chang Lee: *Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method*, International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No 1, 2014.

[Li96] Sharman Lichtenstein: *Factors in the selection of risk assessment method*, Information Management & Computer Security 4/4, S. 20-25, 1996.

[LSS11] Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen: *Model-Driven Risk Analysis*, Springer-Verlag Berlin Heidelberg, 2011.

[Ma14] Spanisches Ministerium für öffentliche Verwaltungen, *MAGERIT V.3 (English version): Methodology for Information Systems Risk Analysis and Management*, 2014, NIPO: 630-14-162-0.

[Mc06] Gary McGraw: *Software Security: Building Security In*, 1st ed., Addison-Wesley, 2006. ISBN-10: 0321356705.

[DR10] DeMeer Jan, Rennoch Axel, *The ETSI TVRA Security-Measurement Methodology by means of TTCN-3 Notation*, 10th TTCN-3 User Conference, 2011.

[Mo12] Rim Moalla et al.: *Risk analysis study of ITS communication architecture*, Third International Conference on the Network of the Future (NOF), S. 1 – 5, 2012.

[Mo09] Ayse Morali et al.: *Extended eTVRA vs. Security Checklist: Experiences in a Value-Web*, 31st International Conference on Software Engineering-Companion Volume (ICSE-Companion), S. 130 – 140, 2009.

[Ms01] Microsoft, *Bedrohungen und Gegenmaßnahmen*, https://msdn.microsoft.com/library/aa302418.aspx zuletzt aufgerufen 22.10.15.

[NIS14] National Institute of Standards and Technology (NIST) Ross R., Oren J., McEvilley M.: *NIST Special Publication 800-160 Initial Public Draft, Systems Security Engineering*, 2014.

[No05] Thomas Nowey et al.: *Ansätze zur Evaluierung von Sicherheitsinvestitionen*, , Beiträge der 2. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. GI-Edition / Proceedings, 62. Ges. für Informatik, Bonn, S. 15-26, 2005, ISBN 3-88579-391-1.

[OWA13] Open Web Application Security Project (OWASP), *OWASP Top 10-2013 Die 10 häufigsten Sciherheitsrisiken für Webanwendungen*, 2013.

[Po04] Hartmut Pohl *Taxonomie und Modellbildung in der Informationssicherheit*, Datenschutz und Datensicherheit, 28, S. 678-685, 2004.

[Ra13] Lisa Rajbhandari: *Consideration of Opportunity and Human Factor: Required Paradigm Shift for Information Security Risk Management*, European Intelligence and Security Informatics Conference, S. 147 – 150, 2013.

[Re12] Frank Reichenbach et al.: *A Pragmatic Approach on Combined Safety and Security Risk Analysis*, 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW), S. 239 – 244, 2012.

[Ro08] Artur Rot: *IT Risk Assessment: Quantitative and Qualitative Approach*, Proceedings of The World Congress on Engineering and Computer Science, S. 1073-1078, 2008, ISBN: 978-988-98671-0-2.

[RCS07] Judith E. Y. Rossebø, Scott Cadzow, Paul Sijben: *eTVRA, a Threat, Vulnerability and Risk Assessment Method and Tool for eEurope*, The Second International Conference on Availability, Reliability and Security (ARES'07), S. 925 – 933, 2007.

[RSH91] Rex Kelly Rainer Jr., Charles A. Snyder, Houston H. Carr: Risk Analysis for Information Technology, Journal of Management Information System, Vol. 8, No.1, S. 129-247, 1991.

[SH03] Bomil Suh, Ingoo Han: *The IS risk analysis based on a business* model, Information & Management 41, S.149–158, 2003.

[SHS09] Amril Syalim Yoshiaki Hori, Kouichi Sakura: *Comparison of Risk Analysis Methods: Mehari, MAGERIT, NIST800-30 and Microsoft's Security Management Guide*, International Conference on Availability, Reliability and Security, S. 726 – 731, 2009.

[Sh14] Adam Shostack: *threat modelling designing for security*, Wiley, 2014. ISBN: 978-1-118-80999-0.

[SK12] Neeta Shukla, Sachin Kumar: A Comparative Study on Information Security Risk Analysis Practices, Issues and Challenges in Networking, Intelligence and Computing Technologies – ICNICT, S. 28-33, 2012.

[Sp09] Janine L. Spears: A Holistic Risk Analysis *Method for Identifying Information Security*, Risks Security Management, Integrity, and Internal Control in Information Systems Volume 193 of the series IFIP International Federation for Information Processing, S. 185-202, 2009, ISBN:978-0-387-31167-8.

[SWH13] Sardar Muhammad Sulaman, Kim Weyns, Martin Höst: *Review of Research on Risk Analysis Methods for IT Systems*, International Conference on Evaluation and Assessment in Software Engineering In Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering, S. 86-96, 2013.

[To02] Toval A. et al.: *Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach* Requirements Engineering, Springer-Verlag London Limited, S. 205-219, 2002.

[VH07] Melanie Volkamer, Harald Hauff: *Zum Nutzen hoher Zertifizierungsstufen nach den Common Criteria (I)*, Datenschutz und Datensicherheit - DuD, Volume 31, Issue 9, Springer, S. 692-695, 2007.

[VL05] Anita Vorster, Les Labuschagne: *A Framework for Comparing Different Information Security Risk Analysis Methodologies*, Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, 2005.

[WL09] Dong Wang, Chen Liu: *Model-based Vulnerability Analysis of IMS Network*, Journal of Networks, Vol. 4, No. 4, Academy Publisher, 2009.

[Ya02] Yazar Z. *Qualitative risk analysis and management tool – CRAMM*, SANS Institute InfoSec Reading Room, 2011.

8 Annex A1

Bodenstation

Bestimmung des Evaluationsgegenstandes

A Sicherheitsumgebung		
a.1 Annahmen		
TVRA-id	**Zusammenfassung**	
a.1.1	Der S/X- Band Downlink wird über unterschiedliche Frequenzen vom Satelliten zur Bodenstation übertragen.	
a.1.2	Die S-Band Daten werden innerhalb des DLR-Campusnetzes übertragen.	
a.1.3	Der Status über die empfangenen X-Band Daten werden über das DLR-Campusnetzwerk übertragen.	
a.1.4	Die verschlüsselten Radardaten werden im internen Netz der Bodenstation zum TSC übertragen.	
a.1.5	Alle Betriebsmittel befinden sich innerhalb kontrollierten Räumlichkeiten, zu denen nur befugte Personen Zugang haben.	
a.1.6	Arbeitsplätze befinden sich innerhalb kontrollierter Räumlichkeiten, zu denen nur	

	befugte Personen Zugang haben.	
a.2 Schützenswerte Güter (assets)		
a.2.1	X-Band Daten = Radardaten	
a.2.2	Empfangsausrüstung	
a.2.3	Antenne	
a.3 Bedrohungen (threats)		
a.3.1	Unbefugter Abruf der Radardaten	
a.3.2	Unbefugte Änderung der Radardaten	
a.3.3	Abhören des Netzverkehrs vom Satelliten zur Bodenstation	
a.3.4	Abhören des Netzverkehrs innerhalb des DLR-Campusnetzes	
a.3.5	Unterbrechung der Kommunikationsbeziehung zwischen dem Satelliten und der Bodenstation	
a.4 Sicherheitspolitik (organisatorisch) optional		
a.4.1	Erhöhter Zutrittsschutz zu Räumlichkeiten	
a.4.2	Zutrittsrecht nur für	

	ausgewählte Mitarbeiter	
a.4.3	Erhöhte Zugriffkontrolle auf die Produktionsrechner	
a.4.4	adäquater Malware Schutz	
a.4.5	Erhöhter Zugangsschutz zu Netzwerkkomponenten	
a.4.6	Redundanz der eingesetzten IT-Systeme	
a.4.7	Verschlüsselung zwischen Satellit und Bodenstationen	

Identifikation der Schutzziele

B Schutzziele (security objectives)		
Schutzziel		
b.1.1	Es muss sichergestellt werden, dass die Radardaten auf den Empfangsrechnern nicht verändert werden können (Integrität).	
b.1.2	Es muss sichergestellt werden, dass die Radardaten bei der Übertragung vom Satelliten zur Bodenstation nicht verändert werden können (Integrität).	
b.1.3	Es muss sichergestellt werden, dass die Radardaten bei der Übertragung vom Satelliten zur Bodenstation nicht abgehört werden können (Vertraulichkeit).	

b.1.4	Es muss sichergestellt werden, dass die Radardaten bei der Übertragung innerhalb des Campusnetzes nicht verändert werden können (Integrität).	
b.1.5	Es muss sichergestellt werden, dass die Radardaten bei der Übertragung innerhalb des DLR-Campusnetzes nicht abgehört werden können (Vertraulichkeit).	
b.1.6	Die Antenne muss funktionsfähig sein, um den Empfang der Daten zu gewährleisten (Verfügbarkeit).	
b.2 Schutzziele für die Umgebung		
b.2.1	Es muss sichergestellt werden, dass nur autorisierte Personen Zugang zu den Empfangsräumen haben (Vertraulichkeit).	
b.2.2	Es muss sichergestellt werden, dass nur autorisierte Personen physischen Zugriff auf die Antenne und die Empfangsrechner haben (Vertraulichkeit).	

Identifikation der funktionalen Sicherheitsanforderungen

C Sicherheitsanforderungen			
c.1 Sicherheitsanforderungen für die schützenswerten Güter			
c.1.1. Funktionale Sicherheitsanforderungen			
c.1.1.1	Der Zugang auf die	Access Control	ISO/IEC 15408-

	Betriebsrechner muss über eine Zugangskontrollfunktion geregelt werden.	Function FDP_ACF	2 S.54
c.1.1.2	Es muss sichergestellt werden, dass die Daten bei der Übertragung vom Satelliten zur Bodenstation verschlüsselt werden.	Internal TOE transfer FDP_ITT	ISO/IEC 15408-2 S.67
c.1.1.3	Die Integrität der Radardaten muss überprüft werden; das Ergebnis des Checks muss angezeigt werden.	Stored data Integrity FDP_SDI	ISO/IEC 15408-2 S.81
c.1.1.4	Es muss sichergestellt werden, dass für den Transfer der Daten ein Schutzmechanismus gegen Offenlegung der Daten vorhanden ist.	Inter-TSF user data confidentiality transfer protection FDP_UCT	ISO/IEC 15408-2 S.83
c.1.1.5	Bei einer bestimmten Anzahl von erfolglosen Authentisierungsversuchen muss der weitere Zugriff auf das Rechnersystem der Bodenstation gesperrt werden. Die Entsperrung muss explizit erfolgen.	Authentication failures FIA_AFL	ISO/IEC 15408-2 S.89
c.1.2. Sicherheitsanforderungen an die Vertrauenswürdigkeit			

c.1.2.1	Die Schnittstellen zwischen der Antenne und der Empfangsausrüstung müssen detailliert dokumentiert und getestet werden.	Functional specification ADV_FSP	ISO/IEC 15408-3 S. 86
c.1.2.2	Für den Betreiber des Systems muss eine detaillierte Beschreibung seiner Vorgehensweise existieren.	Operational User Guidance AGD_OPE	ISO/IEC 15408-3 S.117

Systematische Identifikation der Verwundbarkeit

Identifikation der Schwachstellen

d.1 Schwachstellen (weakness)		
TVRA-id	**Zusammenfassung**	
d.1.1	Unkontrolliertes Ausbreiten der Funkwellen.	
d.1.2	unsichere Kommunikationsverbindung zwischen Antenne und Direkt Archivsystem.	

Identifikation der Verwundbarkeit, hierfür werden die möglichen Angriffe ermittelt

d.2 Verwundbarkeit (vulnerability)		
TVRA-id	**Zusammenfassung**	
d.2.1	Fehlende Möglichkeit, die Funkwellen abzuschirmen.	
d.2.2	Fehlende Schutzzone.	

Identifikation der Angriffsmethoden

d.3 Angriffsmethoden (attack methods)		
TVRA-id	**Zusammenfassung**	
d.3.1	Abhören der Radardaten durch Datenempfang an einer unautorisierten Antenne.	Angreifer platziert einen Empfänger und empfängt unautorisiert die Daten
d.3.2	Man-in-the-Middle Angriff.	Angreifer platziert sich zwischen den beiden Kommunikationspartnern, hört die gesendeten Nachrichten ab und gibt sich zumindest als einer der beiden Kommunikationspartner aus
d.3.3	Anzapfen der Kommunikationsverbindung.	
d.3.4	Datenempfang stören.	Angreifer platziert einen Sender in der Empfangsreichweite der Antenne , dieser stört den Datenempfang der Antenne

Identifikation von Gegenmaßnahmen

f.1 Gegenmaßnahmen		
TVRA-id	**Zusammenfassung**	
f.1.1	Verschlüsseln der Daten des Downlinks.	
f.1.2	Einzäunen der Antenne und der Empfangsanlage.	

f.1.3	Nur autorisierte Personen haben Zugang zum Gelände auf dem sich die Antenne befindet.	
f.1.4	Nur autorisierte Personen haben Zugang zu den Räumen in dem sich die Rechner der Empfangsanlage befinden.	

Transkription Prozessierungssystem

Bestimmung des Evaluationsgegenstandes

A Sicherheitsumgebung		
a.1 Annahmen		
TVRA-id	**Zusammenfassung**	
a.1.1	Die Downlinkinfo-Datei (DLI) mit dem Key wird über das DLR-Campusnetz übertragen.	
a.1.2	Die entschlüsselten Daten liegen für den Zeitraum des Screening auf dem Produktionsrechner	
a.1.3	Der private Schlüssel für das Entschlüsseln des Schlüssels liegt auf einem Produktionsrechner.	
a.1.4	Der Entschlüsselungsschlüssel liegt für die Zeit der Entschlüsselung der	

	Radardaten unverschlüsselt auf einem Produktionsrechner und muss nach der Entschlüsselung sicher gelöscht werden.	
a.1.5	Der öffentliche Schlüssel für das Verschlüsseln des Schlüssels liegt auf einem Produktionsrechner.	
a.1.6	Der verschlüsselte Radardatensatz wird über das DLR Campusnetz per sftp übertragen.	
a.1.7	Die unverschlüsselten Daten werden im internen Netz der Bodenstation übertragen.	
a.2 Schützenswerte Güter (assets)		
a.2.1	Radardaten	
a.2.2	Entschlüsselungsschlüssel	
a.2.3	Privater Schlüssel	
a.2.4	Öffentlicher Schlüssel	
a.2.5	MOS FTP-Server	
a.3 Bedrohungen (threats)		
a.3.1	Unbefugte Änderung des Schlüssels.	
a.3.2	Abhören des Netzverkehrs des DLR–Campusnetzes.	

a.3.3	Ausspähen des privaten Schlüssels.	
a.3.4	Unbefugte Änderung des Entschlüsselungsschlüssels	
a.3.5	Ausspähen des Entschlüsselungsschlüssels.	
a.3.6	Ausfall der Anwendungen zur Entschlüsselung.	
a.4 Sicherheitspolitik (organisatorisch) optional		
a.4.1	Erhöhter Zutrittsschutz zu den Räumlichkeiten. Zutrittsrecht nur für ausgewählte Mitarbeiter.	
a.4.2	Erhöhter Zugangsschutz zu Netzkomponenten.	
a.4.3	Erhöhte Zugriffkontrolle auf den Produktionsrechner.	
a.4.4	Erhöhter Zugangsschutz zu den Firewall Komponenten.	
a.4.5	adäquater Malware Schutz.	

Identifikation der Schutzziele

B Schutzziele (security objectives)		
b.1 Schutzziele		
b.1.1	Es muss sichergestellt werden, dass Dritte den öffentlichen Schlüssel nicht einsehen (Vertraulichkeit).	

b.1.2	Es muss sichergestellt werden, dass der öffentliche Schlüssel bei der Übertragung nicht verändert werden kann (Integrität).	
b.1.3	Es muss sichergestellt werden, dass Dritte den privaten Schlüssel nicht einsehen (Vertraulichkeit).	
b.1.4	Es muss sichergestellt werden, dass der private Schlüssel bei der Übertragung nicht verändert werden kann (Integrität).	
b.1.4	Es muss sichergestellt werden, dass Dritte den Entschlüsselungsschlüssel nicht lesen können (Vertraulichkeit).	
b.1.5	Es muss sichergestellt werden dass der Entschlüsselungsschlüssel bei der Übertragung nicht verändert werden kann (Integrität).	
b.1.6	Es muss sichergestellt werden, dass Dritte die Radardaten nicht lesen können (Vertraulichkeit).	
b.1.7	Es muss sichergestellt werden dass die Radardaten bei der Übertragung nicht verändert werden können (Integrität).	
b.2 Schutzziele für die Umgebung		
b.2.1	Nur autorisierte Personen haben Zugang zu dem Server, auf dem der öffentliche Schlüssel liegt (Vertraulichkeit).	

b.2.2	Nur autorisierte Personen haben Zugang zu dem Server, auf dem der private Schlüssel liegt (Vertraulichkeit).	
b.2.3	Nur autorisierte Personen haben Zugang zu dem Server, auf dem der Entschlüsselungsschlüssel liegt (Vertraulichkeit).	
b.2.4	Nur autorisierte Personen haben Zugang zum dem Raum, in dem sich die Netzwerkkomponenten befinden (Vertraulichkeit).	

Identifikation der funktionalen Sicherheitsanforderungen

C Sicherheitsanforderungen			
c.1 Sicherheitsanforderungen für die schützenswerten Güter			
c.1.1. Funktionale Sicherheitsanforderungen			
c.1.1.1	Nach erfolgreicher Benutzung des Schlüssels zur Entschlüsselung muss der Schlüssel unwiderruflich gelöscht werden.	FCS_CKM.4 Cryptographic key destruction	ISO/IEC 15408-2 S. 51
c.1.1.2	Die Radardaten müssen erfolgreich entschlüsselt werden mittels einer SatDSiG konformen kryptographischen Operation.	FCS_COP.1 Cryptographic operation	ISO/IEC 15408-2 S. 52

c.1.2. Sicherheitsanforderungen an die Vertrauenswürdigkeit			
c.1.2.1.	Die Entwickler des Transkription Prozessierungssystems müssen das System testen und die Testergebnisse dokumentieren.	ATE_FUN.1	ISO/IEC 15408-3 S.161

Systematische Identifikation der Verwundbarkeit

Identifikation der Schwachstellen

d.1 Schwachstellen (weakness)		
TVRA-id	**Zusammenfassung**	
d.1.1	Kommunikationsverbindung zwischen dem FTP-Server von MOS und dem TSC-Rechner.	
d.1.2	Dienste des MOS FTP-Servers.	
d.1.3	Speicherkapazität des DAS.	
d.1.4	Authentisierungsmethode.	

Identifikation der Verwundbarkeit, hierfür werden die möglichen Angriffe ermittelt

d.2 Verwundbarkeit (vulnerability)		
TVRA-id	**Zusammenfassung**	
d.2.1	Unverschlüsseltes FTP-Protokoll bei der Kommunikationsverbindung zwischen MOS-FTP-Server	

	und TSC.	
d.2.2	Offene Ports.	
d.2.3	Speicherkapazität des DAS ist zu klein.	
d.2.4	Unsichere Authentisierungsmethode.	

Identifikation der Angriffsmethoden

d.3 Angriffsmethoden (attack methods)		
TVRA-id	**Zusammenfassung**	
d.3.1	Man-in-the-Middle Angriff.	
d.3.2	Anzapfen der Kommunikationsverbindung.	

Identifikation von Gegenmaßnahmen

e.1 Gegenmaßnahmen		
TVRA-id	**Zusammenfassung**	
e.1.1	Bei der FTP-Übertragung ein gemeinsames Datenverschlüsselungssystem zwischen Client und Server einsetzen.	
e1.2	Unbenutzte Ports schließen.	

Spezifikation von detaillierten Anforderungen

f.1 detaillierte Maßnahmen		
TVRA-id	**Zusammenfassung**	
f.1.1	Nutzung des VSITR-	Dies ist ein Standard vom

	Standards für das Löschen des Entschlüsselungsschlüssels.	BSI, bei dem die Datei insgesamt sieben Male überschrieben wird. Das Zahlenmuster wechselt bei den ersten sechs Überschreibvorgängen. Beim letzten Überschreibungsvorgang wird die binäre Zahlenfolge 01010101 verwendet (siehe [Ha01]).
f.1.2	Für die Entschlüsselung der Daten soll das ein TripleDes-Verfahren, in einem Cipher-Block-Chaining (CBC)-Modus durchgeführt werden.	Hierbei sollen mehrere Blöcke zu einer Kette zusammengefasst werden und für die Ver- bzw. Entschlüsselung 3 -mal der Data Encryption Standard (DES) verwendet werden.

Webschnittstelle

Bestimmung des Evaluationsgegenstandes

A Sicherheitsumgebung		
a.1 Annahmen		
TVRA-id	**Zusammenfassung**	
a.1.1	Der Webserver befindet sich innerhalb einer DMZ.	
a.1.2	Nutzer, die auf die Daten zugreifen wollen, müssen sich zuerst registrieren und werden dann manuell autorisiert.	

a.1.3	Die bestellten Daten werden auf einem FTP-Server innerhalb der DMZ abgelegt.	
a.2 Schützenswerte Güter (assets)		
a.2.1	Nutzerdaten	
a.2.2	Passwörter	
a.2.3	Ausgelieferte Produkte	
a.2.4	Webserver	
a.2.4	FTP-Server	
a.3 Bedrohungen (threats)		
a.3.1.	Unautorisierter Zugriff auf die Nutzerdaten.	
a.3.2	Unautorisierter Zugriff auf das Passwort.	
a.3.3	Unautorisierter Zugriff auf die ausgelieferten Produkte.	
a.3.4	Unterbinden des Datenaustausches sowie der Kommunikation zwischen dem Webserver und den benötigten Servern innerhalb des DLR-LAN.	
a.4 Sicherheitspolitik (organisatorisch) optional		
a.4.1.	Erhöhter Zutrittsschutz zum Raum, in dem der Webserver und der FTP-Server stehen.	

a.4.2	Zutrittsrecht nur für ausgewählte Mitarbeiter.	
a.4.3	Erhöhte Zugriffskontrolle auf den Rechner.	
a.4.4	Adäquater Malware Schutz.	
a.4.5	Erhöhter Zugangsschutz zu Netzkomponenten.	
a.4.6	Redundanz der eingesetzten IT-Systeme.	

Identifikation der Schutzziele

B Schutzziele (security objectives)		
Schutzziele		
b.1.2	Es muss sichergestellt werden, dass die Nutzerdaten nicht verändert werden können (Integrität).	
b.1.2	Es muss sichergestellt werden, dass das Passwort nicht verändert werden kann (Integrität).	
b.1.3	Es muss sichergestellt werden, dass das Passwort nicht eingesehen werden kann (Vertraulichkeit).	
b.1.4	Die Produkte auf dem FTP-Server dürfen nicht verändert werden (Vertraulichkeit).	
b.1.5	Die Produkte auf dem FTP-Server dürfen nicht eingesehen werden (Vertraulichkeit).	
b.1.6	Der Webserver muss funktionsfähig	

	sein, damit die Bedienoberfläche zur Verfügung steht (Verfügbarkeit).	
b.1.7	Der FTP-Server muss funktionsfähig sein, um die Daten ausliefern zu können (Verfügbarkeit).	
b.1.8	Bestelldaten müssen nachweisbar einem Nutzer zugewiesen werden können (Zurechenbarkeit).	
b.1.9	Es muss sichergestellt werden, dass nur registrierte Benutzer Daten bestellen können (Authentizität).	
b.2 Schutzziele für die Umgebung		
b.2.1	Nur autorisierte Personen haben Zugang zu dem Webserver (Vertraulichkeit, Authentizität).	
b.2.2	Nur autorisierte Personen haben Zugang zu dem FTP-Server (Vertraulichkeit, Authentizität).	
b.2.2	Nur autorisierte Personen haben Zugang zum dem Raum, in dem sich die Netzwerkkomponenten befinden (Vertraulichkeit, Authentizität).	

Identifikation der funktionalen Sicherheitsanforderungen

C Sicherheitsanforderungen			
c.1 Sicherheitsanforderungen für die schützenswerten Güter			
c.1.1. Funktionale Sicherheitsanforderungen			
c.1.1.1	Es muss sichergestellt	Non-repudiation of	ISO/IEC 15408-2

	werden, dass der FTP-Server die Daten gesendet hat (Zurechenbarkeit).	origin (FCO_NRO)	S.44
c.1.2	Es muss sichergestellt werden, dass der Empfänger die Daten von dem FTP-Server erhalten hat (Zurechenbarkeit).	Non-repudiation of receipt (FCO_NRR)	ISO/IEC 15408-2 S.45
c.1.3	Es muss sichergestellt werden, dass die Passwörter der registrierten Nutzer nicht eingesehen oder verändert werden.	Stored Data Integrity (FDP_SDI)	ISO/IEC 15408-2 S.74
c.1.4	Es muss sichergestellt werden, dass nach einer definierten Anzahl an fehlgeschlagenen Anmeldeversuchen am Webserver, dieses Vorgehen gemeldet wird.	Authentication failure handling (FIA_AFL.1)	ISO/IEC 15408-2 S.90
c.1.5	Es muss sichergestellt werden, dass der Nutzer sich bei der Anmeldung am Webserver erfolgreich authentisiert, bevor er	User authentication (FIA_UAU)	ISO/IEC 15408-2 S.94

	Zugriff auf Dienste des Webservers bekommt.		
c.1.2. Sicherheitsanforderungen an die Vertrauenswürdigkeit			
c.1.2.1.	Es muss sichergestellt werden, dass der Entwickler des Webservers eine funktionale Spezifikation bereitstellt.	Basic functional specification ADV_FSP.1.1D	ISO/IEC 15408-3 S.90

Systematische Identifikation der Verwundbarkeit

Identifikation der Schwachstellen

d.1 Schwachstellen (weakness)		
TVRA-id	**Zusammenfassung**	
d.1.1	Dienste des FTP-Servers für die Datenauslieferung.	
d.1.2	Dienste des Webservers für die Datenbestellung.	
d.1.3	Kommunikationsverbindung	
d.1.4	Datenzugriffskomponente	
d.1.5	HTTP Cookies	
d.1.6	HTTP Anfragen	
d.1.7	Nutzername	
d.1.8	Passwörter	
d.1.9	Netzkomponenten	

d.1.10	Inputdaten werden zurück an den Browser gesendet.	
d.1.11	Session-Id	
d.1.12	Ports	
d.1.13	Direkte Objektreferenzen	
d.1.14	Weiterleiten	
d.1.15	ICMP	

Identifikation der Verwundbarkeit, hierfür werden die möglichen Angriffe ermittelt

d.2 Verwundbarkeit (vulnerability)		
TVRA-id	**Zusammenfassung**	
d.2.1	Unsichere Passwörter	
d.2.2	Fehlende Schutzzone	
d.2.3	Fehlende Timeoutfunktion	
d.2.4	Offene Ports beim Webserver.	
d.2.5	Offene Ports beim FTP-Server.	
d.2.6	Benutzen eines Benutzerauthentisierungsprozesses (mit bekannten Schwachstellen).	
d.2.7	Verwenden von http Cookies.	
d.2.8	Benutzerkonten mit unnötigen Rechten.	
d.2.9	Statuslosigkeit des http-Protokolls.	
d.2.10	Nicht überprüfen von http-Anfragen.	
d.2.10	Unzureichender Identitätscheck.	
d.2.11	Fehlerhafte	

	Autorisierungsmethode auf der Anwendungsebene.	
d.2.12	Anwendung, die eine Weiterleitung benutzt.	
d.2.13	Web-Anwendung nutzt direkte Objektreferenzen, ohne die Berechtigung des Nutzers zu überprüfen.	

Identifikation der Angriffsmethoden

d.3 Angriffsmethoden (attack methods)		
TVRA-id	**Zusammenfassung**	
d.3.1	SYN-Flood (DoS oder DDoS-Angriff).	Der Angriff verwendet den Verbindungsaufbau des TCP-Transportprotokolls, um einzelne Dienste oder ganze Computer aus dem Netzwerk unerreichbar zu machen. Bei einem DoS-Angriff wird ein Server mit sehr vielen Anfragen bombardiert, wodurch der Server mit der Abarbeitung der Anfragen so sehr aus- bzw. gar überbelastet ist, dass er normale Anfragen nicht mehr bedienen kann.
d.3.2	Man-in-the-Middle Angriff.	Angreifer platziert sich zwischen den beiden Kommunikationspartnern, hört die gesendeten

		Nachrichten ab und gibt sich zumindest als einer der beiden Kommunikationspartner aus.
d.3.4	Identitätsdiebstahl => illegale Registrierung von einem Angreifer beim Webserver.	
d.3.5	Verändern der Daten auf dem Kommunikationsweg.	
d.3.6	Durch Erraten oder systematischer Erprobung des Passwortes kann sich ein Angreifer als legaler Nutzer ausgeben.	Durch Zugriff als legaler Nutzer auf den Webserver, kann der Angreifer die Daten des Nutzers ändern oder illegale Bestellungen von Daten aufgeben, die dem Nutzer in Rechnung gestellt werden.
d.3.7	Cross-Site Scripting.	Bei einer Anfrage an den Webserver werden ausführbare Codeteile übermittelt. Dieser Code kann den Speicherbereich des Severs infizieren oder als Antwort an den Client zurückgeschickt werden und dort ausgeführt werden.
d.3.8	Cross-Site Request Forgery (CRF).	Angreifer kann eine Transaktion über eine Webanwendung durchführen: Hierfür muss ein Nutzer angemeldet sein, seinem

		Webbrowser wird ohne dessen Wissen eine arglistige HTTP-Anforderung untergeschoben.
d.3.9	Angreifer kann durch Änderungen eines Parameters auf Objekte zugreifen	
d.3.10	Portscan	Die ist kein Angriff im eigentlichen Sinn. Hierdurch kann das Netzwerk und der Zustand eines Rechners untersucht werden. Die erhaltenen Informationen sind wichtig für einen möglichen Angriff
d.3.11	Session Hijacking	

Identifikation von Gegenmaßnahmen

e.1 Gegenmaßnahmen		
TVRA-id	**Zusammenfassung**	
e.1.1	Verschlüsseln der Daten.	
e.1.2	Schließen der offenen Ports.	
e.1.3	Kommunikation verschlüsseln; Verwenden von SSL, um einen verschlüsselten Kanal bereitzustellen.	
e.1.4	Einsatz einer Firewall.	

e.1.5	Einsatz von Passwortrichtlinien.	
e.1.6	Weise Nutzern minimale Rechte zu.	
e.1.7	Überwachen typischer Kennwerte, wie Netzwerkauslastung oder Speicherauslastung. Dies ermöglicht eine zeitnahe Alarmierung und Einleitung von Reaktionen.	
e.1.8	Neueste Version der Zugangskomponente nutzen.	
e.1.9	Indirekte Objektreferenz verwenden.	
e.1.10	Jede Eingabeseite sollte einen Token beinhalten, welcher einzigartig ist und vom Server geprüft werden sollte.	

9 Annex A2

Risikoabschätzung

Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
A Abhören der Radardaten durch Datenempfang an einer unautorisierten Antenne	Zeit	4: <= 1 Monat	Mehr als Hoch	Unwahrscheinlich	Hoch	Bedeutend
	Expertise	5: Experten				
	Kenntnisse	4: Sensibel				
	Gelegenheit	12: Schwer				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	3: Hoch				
	Intensität	1:Wenige verschiedene Angriffsinstanzen				

Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		

A Anzapfen der Kommunikationsverbindung zwischen der Antenne und der Empfangsausrüstung	Zeit	1: <= 1 Woche	Mehr als Hoch	Unwahrscheinlich	Hoch	Bedeutend
	Expertise	5: Experten				
	Kenntnisse	10: Kritisch				
	Gelegenheit	12: Schwer				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	3: Hoch				
	Intensität	1:Wenige verschiedene Angriffsinstanzen				

Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
A Datenempfang stören	Zeit	0: <= 1 Tag	Einfach	Wahrscheinlich	Hoch	Kritisch
	Expertise	2: Profis				
	Kenntnisse	0: Öffentlich				
	Gelegenheit	1: Einfach				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	3: Hoch				

	Intensität	0:Eine Angriffsinstanz				

Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
A Man-in-the-Middle Angriff zwischen der Antenne und der Empfangsausrüstung	Zeit	2: <= 2 Wochen	Moderat	Möglich	Hoch	Kritisch
	Expertise	5: Experten				
	Kenntnisse	0: Öffentlich				
	Gelegenheit	0: Nicht erforderlich/ uneingeschränkter Zugriff				
	Ausrüstung	0: Standard				
	Auswirkungen auf das schützenswerte Gut	3: Hoch				
	Intensität	0:Eine Angriffsinstanz				

Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
B Anzapfen der Kommunikationsverbindung zwischen MOS-FTP-Server und TSC	Zeit	0: <= 1 Tag	Moderat	Möglich	Gering	Gering
	Expertise	2: Profis				
	Kenntnisse	0: Öffentlich				

	Gelegenheit	4: Moderat				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	1: Niedrig				
	Intensität	0:Eine Angriffsinstanz				
Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
B Man-in-the-Middle Angriff zwischen MOS-FTP-Server und TSC	Zeit	0: <= 1 Tag	Moderat	Möglich	Gering	Gering
	Expertise	2: Profis				
	Kenntnisse	0: Öffentlich				
	Gelegenheit	4: Moderat				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	1: Niedrig				
	Intensität	0:Eine Angriffsinstanz				
Threat Group	**Angriff**				**Auswirkungen**	**Risiko**

	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Cross-Site Request Forgery (Angreifer generiert eine gefälschte HTTP-Anfrage)	Zeit	0: <= 1 Tag	Einfach	Wahrscheinlich	Mittel	Kritisch
	Expertise	2: Profis				
	Kenntnisse	1: Eingeschränkt				
	Gelegenheit	1: Einfach				
	Ausrüstung	0: Standard				
	Auswirkungen auf das schützenswerte Gut	2: Mittel				
	Intensität	0:Eine Angriffsinstanz				
Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Erraten oder systematisches Ausprobieren des Passwortes	Zeit	4: <= 1 Monat	Moderat	Möglich	Mittel	Bedeutend
	Expertise	2: Profis				
	Kenntnisse	4: Sensibel				
	Gelegenheit	1: Einfach				
	Ausrüstung	0: Standard				
	Auswirkungen auf das schützenswerte	2: Mittel				

	Gut					
	Intensität	0:Eine Angriffsinstanz				
Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Identitätsdiebstahl => illegale Registrierung von einem Angreifer beim Webserver	Zeit	0: <= 1 Tag	Moderat	Möglich	Mittel	Bedeutend
	Expertise	2: Profis				
	Kenntnisse	4: Sensibel				
	Gelegenheit	1: Einfach				
	Ausrüstung	0: Standard				
	Auswirkungen auf das schützenswerte Gut	2: Mittel				
	Intensität	0:Eine Angriffsinstanz				
Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Man-in-the-Middle Angriff zwischen FTP-Server und	Zeit	0: <= 1 Tag	Moderat	Möglich	Mittel	Bedeutend
	Expertise	2: Profis				

Rechner eines legalen Benutz	*Kenntnisse*	1: Eingeschränkt				
	Gelegenheit	1: Einfach				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	2: Mittel				
	Intensität	0:Eine Angriffsinstanz				

Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Nutzen der Software mit bekannten Schwachstellen=> illegale Registrierung	Zeit	0: <= 1 Tag	Moderat	Möglich	Hoch	Kritisch
	Expertise	2: Profis				
	Kenntnisse	0: Öffentlich				
	Gelegenheit	1: Einfach				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	3: Hoch				
	Intensität	2:Viele verschiedene Angriffsinstanzen				

Threat Group	Angriff				Auswirkungen	Risiko
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Nutzen von Anwendungen mit Weiterleitung um Schadsoftware zu installieren oder	Zeit	1: <= 1 Woche	Einfach	Wahrscheinlich	Hoch	Kritisch
	Expertise	2: Profis				
	Kenntnisse	1: Eingeschränkt				
	Gelegenheit	1: Einfach				
	Ausrüstung	0: Standard				
	Auswirkungen auf das schützenswerte Gut	3: Hoch				
	Intensität	0:Eine Angriffsinstanz				

Threat Group	Angriff				Auswirkungen	Risiko
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Portscan	Zeit	0: <= 1 Tag	keine Bewertung	Wahrscheinlich	Gering	Bedeutend
	Expertise	0: Laie				
	Kenntnisse	0: Öffentlich				
	Gelegenheit	0: Nicht erforderlich/ uneingeschränkter Z				

	Ausrüstung	0: Standard				
	Auswirkungen auf das schützenswerte Gut	1: Niedrig				
	Intensität	0:Eine Angriffsinstanz				
Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Session-Hijacking	Zeit	0: <= 1 Tag	Moderat	Möglich	Hoch	Kritisch
	Expertise	5: Experten				
	Kenntnisse	0: Öffentlich				
	Gelegenheit	1: Einfach				
	Ausrüstung	0: Standard				
	Auswirkungen auf das schützenswerte Gut	2: Mittel				
	Intensität	1:Wenige verschiedene Angriffsinstanzen				
Threat Group	**Angriff**				**Auswirkungen**	**Risiko**
	Einflussfaktor	**Wert**	**Möglichkeit**	**Wahrscheinlichkeit**		
C Syn-Flood (DoS oder	Zeit	1: <= 1 Woche	Moderat	Möglich	Hoch	Kritisch

DDoS)	*Expertise*	2: Profis				
	Kenntnisse	0: Öffentlich				
	Gelegenheit	1: Einfach				
	Ausrüstung	3: Spezialisiert				
	Auswirkungen auf das schützenswerte Gut	3: Hoch				
	Intensität	2:Viele verschiedene Angriffsinstanzen				

Gegenmaßnahmen-Kosten-Nutzen-Tabelle

Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
A Einzäunen der Antenne und der Empfangsanlage	**Standard-Ausbau**	Mittlere Auswirkung	**Gering**	2	1	1
	Umsetzung	Mittlere Auswirkung	**Bedeutend**	2	2	
	Betrieb	Keine Auswirkung	**Kritisch**	0	0	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		

Gegenmaßnahme	Kosten		Nutzen			Ergebnis
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
A Nur autorisierte Personen haben Zugang zu dem Gelände auf dem sich die Antenne befindet	**Standard-Ausbau**	Keine Auswirkung	**Gering**	1	0	19
	Umsetzung	Keine Auswirkung	**Bedeutend**	1	1	
	Betrieb	Keine Auswirkung	**Kritisch**	2	0	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		

Gegenmaßnahme	Kosten		Nutzen			Ergebnis
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
A Nur autorisierte Personen haben Zugang zu den Räumen der Empfangsanlage	**Standard-Ausbau**	Mittlere Auswirkung	**Gering**	4	2	14
	Umsetzung	Mittlere Auswirkung	**Bedeutend**	4	1	
	Betrieb	Geringe Auswirkung	**Kritisch**	0	0	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		

Gegenmaßnahme	Kosten		Nutzen			Ergebnis
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
B Bei der FTP-Übertragung ein gemeinsames	**Standard-Ausbau**	Geringe Auswirkung	**Gering**	0	0	0

Datenverschlüsselungssystem nutzen	**Umsetzung**	Geringe Auswirkung	**Bedeutend**	2	2	
	Betrieb	Keine Auswirkung	**Kritisch**	2	2	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
B Schließen von nicht benutzen Ports	**Standard-Ausbau**	Keine Auswirkung	**Gering**	3	2	-3
	Umsetzung	Keine Auswirkung	**Bedeutend**	3	4	
	Betrieb	Keine Auswirkung	**Kritisch**	2	2	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Überwachen typischer Kennwerte, wie Netzwerkauslastung oder Speicherauslastung	**Standard-Ausbau**	Geringe Auswirkung	**Gering**	0	0	0
	Umsetzung	Geringe Auswirkung	**Bedeutend**	0	0	
	Betrieb	Mittlere Auswirkung	**Kritisch**	0	0	
	Behördliche Auswirkungen			Keine Auswirkung		

	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Benutze zentralen Mechanismus für die Authentifizierung	**Standard-Ausbau**	Geringe Auswirkung	**Gering**	2	0	10
	Umsetzung	Geringe Auswirkung	**Bedeutend**	2	0	
	Betrieb	Keine Auswirkung	**Kritisch**	20	20	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Benutzen der aktuellsten Version der verwendeten Software	**Standard-Ausbau**	Geringe Auswirkung	**Gering**	5	4	9
	Umsetzung	Geringe Auswirkung	**Bedeutend**	3	1	
	Betrieb	Mittlere Auswirkung	**Kritisch**	0	0	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	

C Benutzen von starken Passwortrichtlinien	**Standard-Ausbau**	Keine Auswirkung	**Gering**	10	8	38
	Umsetzung	Keine Auswirkung	**Bedeutend**	4	4	
	Betrieb	Mittlere Auswirkung	**Kritisch**	5	1	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Einsatz einer Firewall	**Standard-Ausbau**	Geringe Auswirkung	**Gering**	6	6	0
	Umsetzung	Geringe Auswirkung	**Bedeutend**	7	7	
	Betrieb	Keine Auswirkung	**Kritisch**	23	23	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Jede Webseite sollte einen einzigartigen Token besitzen	**Standard-Ausbau**	Mittlere Auswirkung	**Gering**	3	0	47
	Umsetzung	Mittlere Auswirkung	**Bedeutend**	12	10	
	Betrieb	Keine Auswirkung	**Kritisch**	4	0	

	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Setze httponly-Flag um das Lesen und Manipulieren der Daten zu verhindern	**Standard-Ausbau**	Geringe Auswirkung	**Gering**	0	0	0
	Umsetzung	Geringe Auswirkung	**Bedeutend**	0	0	
	Betrieb	Keine Auswirkung	**Kritisch**	0	0	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Nicht überprüftes Weiterleiten deaktivieren	**Standard-Ausbau**	Mittlere Auswirkung	**Gering**	2	2	0
	Umsetzung	Mittlere Auswirkung	**Bedeutend**	4	4	
	Betrieb	Keine Auswirkung	**Kritisch**	1	1	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**

	Kategorie	Wert	Risikolevel	ursprüngliche Anzahl	verbesserte Anzahl	
C Verwenden von indirekte Objektreferenzen	**Standard-Ausbau**	Mittlere Auswirkung	**Gering**	1	0	14
	Umsetzung	Mittlere Auswirkung	**Bedeutend**	1	0	
	Betrieb	Keine Auswirkung	**Kritisch**	1	0	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		
Gegenmaßnahme	**Kosten**		**Nutzen**			**Ergebnis**
	Kategorie	**Wert**	**Risikolevel**	**ursprüngliche Anzahl**	**verbesserte Anzahl**	
C Weise Nutzern minimale Rechte zu	**Standard-Ausbau**	Geringe Auswirkung	**Gering**	5	5	147
	Umsetzung	Keine Auswirkung	**Bedeutend**	18	6	
	Betrieb	Geringe Auswirkung	**Kritisch**	12	1	
	Behördliche Auswirkungen			Keine Auswirkung		
	Marktakzeptanz			Keine Auswirkung		

Erklärung

Name: Silke Kerkhoff

Matrikel-Nr.: 7499221

Fach: Praktische Informatik

Modul: Masterarbeit

Ich erkläre, dass ich die vorliegende Abschlussarbeit mit dem Thema

Anwendung und Untersuchung einer Methode zur Analyse von

IT-Sicherheitsrisiken

anhand eines hochwertigen Erdfernerkundungssystems

selbstständig und ohne unzulässige Inanspruchnahme Dritter verfasst habe. Ich habe dabei nur die angegebenen Quellen und Hilfsmittel verwendet und die aus diesen wörtlich, inhaltlich oder sinngemäß entnommenen Stellen als solche den wissenschaftlichen Anforderungen entsprechend kenntlich gemacht. Die Versicherung selbstständiger Arbeit gilt auch für Zeichnungen, Skizzen oder graphische Darstellungen. Die Arbeit wurde bisher in gleicher oder ähnlicher Form weder derselben noch einer anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht. Mit der Abgabe der elektronischen Fassung der endgültigen Version der Arbeit nehme ich zur Kenntnis, dass diese mit Hilfe eines Plagiatserkennungsdienstes auf enthaltene Plagiate überprüft und ausschließlich für Prüfungszwecke gespeichert wird.

Datum: _____ Unterschrift: _____