GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Fraunhofer
IESE

Secure and Safe Microkernel Made in Germany: Kriterien und Konzepte für eine modulare Security-Zertifizierung Safety-kritischer Virtualisierungs-plattformen

Schlussbericht des IESE-Teilprojekts im SeSaM-Verbundvorhaben

Dieses Teilprojekt wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01BY1123 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Fördergeber:	Bundesministerium für Bildung und Forschung
Förderkennzeichen:	01BY1123
Projektlaufzeit:	01.04.2011 – 31.03.2013
Projektpartner:	SYSGO AG, Klein-Winternheim (Konsortialführer) Deutsches Forschungszentrum für Künstliche Intelligenz, Saarbrücken EADS Deutschland GmbH – EADS Innovation Works, München

Autor

Reinhard Schwarz

IESE-Report No. 026.13/D
Version 1.0
Mai 2013

Eine Publikation des Fraunhofer IESE

Das Fraunhofer IESE ist ein Institut der Fraunhofer-Gesellschaft.

Das Institut transferiert innovative Software-Entwicklungstechniken, -Methoden und -Werkzeuge in die industrielle Praxis. Es hilft Unternehmen, bedarfsgerechte Software-Kompetenzen aufzubauen und eine wettbewerbsfähige Marktposition zu erlangen.

Das Fraunhofer IESE steht unter der Leitung von

Prof. Dr. Dieter Rombach (geschäftsführend)
Prof. Dr. Peter Liggesmeyer
Fraunhofer-Platz 1
67663 Kaiserslautern

Kurzfassung

Der vorliegende Bericht fasst den Verlauf und die Ergebnisse des Teilprojekts »Kriterien und Konzepte für eine modulare Security-Zertifizierung Safety-kritischer Virtualisierungsplattformen« im Rahmen des SeSaM Verbundvorhabens zusammen. Er bildet den Schlussbericht des Teilprojekts.

Das Verbundvorhaben »Secure and Safe Microkernel Made in Germany« (SeSaM) ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Forschungsprojekt. Es wurde gemeinsam von den Forschungspartnern SYSGO, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), EADS Innovation Works und Fraunhofer IESE mit einer Projektlaufzeit von 24 Monaten durchgeführt.

Das Ziel des Vorhabens war es, Grundlagen für die Entwicklung und Zertifizierung hochsicherer Betriebssystemkomponenten zu schaffen, auf denen Anwendungen unterschiedlicher Sicherheitskritikalität ablaufen. Dabei wurde ein Maß an Informationssicherheit (Security) angestrebt, das hohen und höchsten Assurance Levels der Common Criteria for IT Security Evaluation sowie einschlägigen Safety-Normen wie etwa DO-178C/ED-12C genügt.

Fraunhofer IESE trug zu diesem Vorhaben vor allem mit Konzepten und Methoden für eine modulare Sicherheitsevaluierung von Separierungskern und darauf aufsetzenden Anwendungen bei. Am Beispiel eines Avionik Security Gateways, das auf einer mikrokernbasierten Virtualisierungsplattform läuft, wurden konzeptionelle Grundlagen für eine modulare Sicherheitszertifizierung erarbeitet. Die entwickelte Methodik wurde angewendet, um am konkreten Beispiel eine systematische Spezifikation des Sicherheitsproblems und darauf aufbauend eine Herleitung der Sicherheitsanforderungen zu erproben.

Dieser Bericht beschreibt Projektrahmen, Konzept und Methodik des im Projekt entwickelten modularen Evaluierungsansatzes und diskutiert die im Vorhaben gewonnenen Einsichten.

Schlagwörter: Informationssicherheit, modulare Zertifizierung, Separierungskern, Common Criteria

Inhaltsverzeichnis

1 Aufgabenstellung

Das Verbundvorhaben »Secure and Safe Microkernel Made in Germany« (SeSaM) ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Forschungsprojekt. Es wurde gemeinsam von den Forschungspartnern SYSGO, Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI), EADS Innovation Works und Fraunhofer IESE mit einer Projektlaufzeit von 24 Monaten durchgeführt.

Das hier beschriebene Teilvorhaben des Fraunhofer IESE war in den größeren Kontext des SeSaM-Verbundvorhabens eingebettet.

1.1 Zielsetzung des SeSaM Verbundvorhabens

Ziel des SeSaM-Projekts war es, Grundlagen für die Entwicklung und Zertifizierung von hochsicheren Betriebssystemkernen zu schaffen. Insbesondere ging es um Virtualisierungslösungen für zentralisierte Plattformen, auf denen Anwendungen unterschiedlicher Kritikalität ablaufen.

Im Kern ging es darum, die Sicherheitsfunktionalitäten solcher Separierungskerne in geeigneter Form zu definieren und auf Basis dieser Spezifikation modulare Verifikationsverfahren zu konzipieren. Spezifikation und Verfahren wurden exemplarisch auf eine konkrete Implementierung eines mikrokernbasierten Separierungskerns (PikeOS der Firma SYSGO) mit einer darauf laufenden sicherheitskritischen Applikationssoftware angewendet und daran erprobt. Dabei wurde eine Zertifizierung der Separierungslösung nach Evaluation Assurance Level (EAL) 4+ der *Common Criteria for Information Technology Security Evaluation* [CC12] angestrebt. Durch geeignete formale Modellierung sollten überdies die Grundlagen für eine mögliche Zertifizierung nach noch höheren Evaluierungsstufen (EAL5/6/7) der Common Criteria (CC) geschaffen werden.

1.2 Zielsetzung des IESE-Teilvorhabens

Das Ziel des von Fraunhofer IESE durchgeführten Teilvorhabens war es, im Projekt vor allem zu den konzeptionellen Grundlagen einer modularen Sicherheitszertifizierung beizutragen. Über den konkreten Anwendungsfall der Systemlösung des Partners SYSGO hinaus war dem Institut vornehmlich an den grundlegenden Security-, Safety- und Qualitätssicherungsanforderungen sowie den dazu passenden Evaluierungstechniken gelegen, die sich auf ähnliche Zertifizierungsprobleme im Software Engineering übertragen lassen.

Die im SeSaM-Projekt zu erarbeitenden Spezifikationen und Prüfverfahren sollten Beiträge zu einem Methodenbaukasten für die Konstruktion und

Zertifizierung sicherheitskritischer Software-Komponenten liefern. Der vorliegende Anwendungsfall einer mikrokernbasierten Separierungslösung war hierzu ein besonders reizvolles Studienobjekt, denn solche Systeme werden gleichermaßen in eingebetteter Software (z.B. in der Avionik) und in der klassischen Informationsverarbeitung (z.B. im Cloud-Computing) eingesetzt, um unterschiedliche Anwendungen oder Anwender sicher voneinander zu trennen.

Aus dieser grundlegenden Zielsetzung leiteten sich folgende konkrete Teilziele und Fragestellungen für das Teilprojekt des Fraunhofer IESE ab:

- *Ermittlung der notwendigen und hinreichenden Security-Anforderungen an allgemeine Separierungslösungen und deren Entwicklungsprozesse:* Welche Eigenschaften werden benötigt, um das Entwurfsziel »Sichere Trennung unabhängiger Programmausführungen auf einer gemeinsamen Plattform« zu gewährleisten? Wie lassen sich diese implementierungsunabhängig und möglichst wiederverwendbar beschreiben? Welche Abstraktionen werden benötigt, um diese Security-Eigenschaften und deren Nachweis möglichst einfach darzustellen?
- *Separierung von Zertifizierungsebenen:* Wie müssen die grundlegenden Sicherheitsgarantien einer Separierungsschicht aussehen, um daraus Security-Nachweise für die darauf aufbauende Anwendung abzuleiten? Was wären generell wichtige Security-Anforderungen einer Anwendungsschicht, die sich auf der Ebene des Separierungskerns sinnvoll erfüllen und verifizieren lassen?

Diese Fragestellungen sollten am Beispiel eines auf dem PikeOS-Mikrokern basierenden Avionik-Gateways gemeinschaftlich mit den anderen SeSaM-Verbundpartnern untersucht werden. Im Ergebnis sollten mit den im Teilvorhaben entwickelten Konzepten zusammen mit den Partnern der Kern der erforderlichen Spezifikationen erstellt werden, die eine Zertifizierung der Separierungslösung nach den Anforderungen der CC (EAL4+ oder höher) ermöglichen.

2 Durchführungsvoraussetzungen für das Vorhaben

Den Rahmen zur Durchführung des IESE-Teilvorhabens lieferte das SeSaM-Verbundvorhaben, an dem neben Fraunhofer IESE noch SYSGO als Konsortialführer, das DFKI und EADS Innovation Works beteiligt waren. Zur Beschreibung der Kompetenzverteilung im Projektkonsortium sein an dieser Stelle auf den Schlussbericht des Gesamtprojekts [Sysgo13], Abschnitt 1.2, verwiesen.

2.1 Planung des Vorhabens

Im Gesamtprojekt waren folgende Arbeitspakete geplant:

- AP1: Generische Sicherheitsanforderungen an Separierungslösungen
- AP2: Sicherheitsvorgaben für den Separierungskern (Security Target)
- AP3: Spezifikation der Sicherheitsarchitektur eines Separierungskerns
- AP4: Modulare Zertifizierung eines zusammengesetzten Systems
- AP5: Formale Sicherheitsmodellierung der Informationsflüsse
- AP6: Prä-Evaluierung des Separierungskerns auf Basis von AP2 und AP3

Eine Gesamtdarstellung der Arbeitspaketziele und der jeweils erzielten Projektergebnisse ist dem Schlussbericht des Gesamtprojekts [Sysgo13] zu entnehmen.

Tabelle 1 Beiträge des IESE-Teilvorhabens zum SeSaM-Verbundvorhaben

Aufgabe	2011									2012												2013		
	Quartal 2			Quartal 3			Quartal 4			Quartal 1			Quartal 2			Quartal 3			Quartal 4			Quartal 1		
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
AP1 — Protection Profile																								
D1.1: Entwurf eines Schutzprofiles	0,5	0,5	0,5	0,5	0,5	0,5																		
D1.2: High-Level Rationale für den Inhalt des Schutzprofils																								
AP2 — Security Target																								
D2.1: Security Target für PikeOS (Pflichtenheft)																								
AP3 — Sicherheitsarchitektur																								
D3.1: Beschreibung der Sicherheitsarchitektur (ADV_ARC)																								
D3.2: Funktionale Spezifikation (ADV_FSP),																								
D3.3: Beschreibung des Softwaredesigns (ADV_TDS)																								
D3.4: Rechtfertigung des Softwaredesigns (ADV_INT)																								
AP4 — Modulare Sicherheitsevaluation																								
D4.1: Security Problem Definition/ Demonstrator																								
D4.2: ST Composite																			1	1	1	1	1	
D4.3: Anwendung der AGD Familie																								
AP5 — Formale Modellierung																								
D5.1: Formales Modell																								
AP6— Prä-Evaluation																								
D6.1: ETR für EAL4+																						1		
D6.2: Gap-Analyse zu EAL6																								
Aufwand IESE (Personenmonate)	3									3												3		
	9																							

Tabelle 1 zeigt die geplante Einbettung der IESE-Teilaufgaben und -aufwände in den Gesamtprojektplan. Gemäß Tabelle 1 war das Teilprojekt planmäßig an folgenden Arbeitspaketen und Ergebnissen (Deliverables) beteiligt:

- **AP1 — Protection Profile:**
  D1.1 Entwurf eines Schutzprofile-Grundgerüsts für Separierungskerne
- **AP4 — Modulare Sicherheitsevaluation:**
  D4.2 Skizze eines Composite Security Targets für ein modulares Beispielsystem
- **AP6 — Prä-Evaluation:**
  D6.1 Beiträge zum Evaluation Technical Report.

Wie der Tabelle zu entnehmen ist, war eine Beteiligung des Fraunhofer IESE an den Arbeitspaketen AP2, AP3 und AP5 nach dem Projektplan nicht vorgesehen, ebenso wenig an den Deliverables D1.2, D2.1, D3.1–3.4, D4.1, D4.3, D5.1 und D6.2. Dies spiegelt den im Vergleich zu anderen Verbundpartnern geringen Projektaufwand wider, der dem Fraunhofer-Institut für das Teilprojekt zur Verfügung stand.

2.2 Ablauf des Vorhabens

Innerhalb des eigenen Teilprojekts arbeitete Fraunhofer IESE vor allem mit dem Forschungspartner DFKI zusammen, der ein akkreditiertes CC-Prüflabor betreibt und daher mit den Common Criteria und deren Qualitätsanforderungen bestens vertraut ist. Da im Rahmen des Teilprojekts Zertifizierungsartefakte nach Common Criteria zu erstellen waren, nutzte das IESE den fachlichen Rat des DFKI in Fragen der standardkonformen Gestaltung von CC-Spezifikationen.

Für die Konzeption und exemplarische Anwendung einer modularen Zertifizierung bezog sich das IESE-Teilprojekt auf den Projektpartner EADS, der ein modular aufgebautes Avionik-Gateway als Anwendungsbeispiel bereitstellte und die Erhebung der dafür relevanten Sicherheitsvorgaben unterstützte.

Während der Anforderungsanalyse erhielt Fraunhofer IESE Impulse von den Industrie- und Anwendungspartnern SYSGO und EADS. Sie sind am besten mit den Marktanforderungen vertraut und konnten daher wertvollen Input zu relevanten Sicherheitsvorgaben liefern.

Während der Anforderungsanalyse zur Schutzprofil-Skizze in Arbeitspaket 1 wurde schnell klar, dass das Schutzprofil (Deliverable D1.1 in AP1) sehr eng mit dem Security Target (Deliverable D2.1 in AP2) verknüpft ist. Daraufhin wurde im Projektkonsortium einvernehmlich beschlossen, beide Deliverables in einem gemeinsamen Dokument zu verwalten, um die übereinstimmenden Bestandteile duplikatfrei nur einmal zu pflegen. Die jeweils artefaktspezifischen Abschnitte wurden durch entsprechende Kommentare gekennzeichnet. Dadurch ergab sich eine sehr enge Kooperation zwischen den Arbeitspaketen AP1 und AP2. Einzelne Beiträge waren schließlich nicht mehr eindeutig nach Arbeitspaketen

abgrenzbar. Infolgedessen arbeitete das Fraunhofer IESE im Rahmen seines Teilprojekts auch mit begrenzten Aufwänden an AP2 mit, obgleich dies im ursprünglichen Projektplan nicht vorgesehen war. Abgesehen davon folgte der Verlauf des Projekts dem ursprünglichen Projektplan.

Während der Projektlaufzeit gab es drei Projekttreffen mit Beteiligung des Fraunhofer IESE, eines zum Projektauftakt in Mainz im Projektmonat M2, ein weiteres in Kaiserslautern im Monat M8 sowie eines im Projektmonat M17 in Saarbrücken. Außerdem trafen sich alle Projektpartner anläßlich eines zweitägigen Projektstatusseminars, das vom Projektträger zur Berichterstattung über die geförderten Forschungsvorhaben veranstaltet wurde, in Projektmonat M18 in Bochum. Neben diesen Treffen erfolgte die weitere projektübergreifende Koordination des Verbundvorhabens durch monatliche Telefonkonferenzen mit allen Projektpartnern sowie durch ein gemeinsam genutztes Projekt-Repository, in dem alle Partner ihre Zwischen- und Endergebnisse für die Verbundmitglieder bereitstellten.

2.3 Verwendete Informations- und Dokumentationsdienste

Im Laufe des Projekts wurden einschlägige Fachpublikationen (z. B. IEEE- und ACM Journals) und Konferenzen (z.T. durch aktive Teilnahme von Verbundprojektpartnern) in üblicher Form verfolgt. Als weitere Quelle diente das Common Criteria Portal [CC], das die aktuelle Fassung der CC sowie begleitende Dokumente und Richtlinien bereithält.

Für die schnelle Beschaffung weiterer vielversprechender Veröffentlichungen diente vor allem das Internet. Abgesehen von einigen kostenpflichtigen Standards waren fast alle benötigten Dokumente entweder kostenfrei beziehbar oder befanden sich bereits im Besitz eines der Verbundpartner.

2.4 Zusammenarbeit mit anderen Stellen

Im SeSaM-Projekt wurden keine Unteraufträge an Dritte vergeben. Eine Zusammenarbeit mit Partnern außerhalb des Projektverbunds war nur insofern vorgesehen, als das Verbundvorhaben von externen Fachexperten Rückmeldung zu vorliegenden Zwischenergebnissen und Anregungen zu praxisrelevanten Aspekten einholte.

So wurden zum Beispiel verschiedene Spezifikationen EADS-Fachleuten außerhalb des Projekts zur Kommentierung vorgelegt. Darüber hinaus wurden die im Verbundvorhaben entwickelten Ideen auf den besuchten Fachkonferenzen intensiv mit anderen Konferenzteilnehmern diskutiert. Eine genauere Übersicht über diese Aktivitäten und den wissenschaftlichen Austausch der SeSaM-Partner findet sich im Schlussbericht des Gesamtprojekts [Sysgo13] im Abschnitt 1.5.

3 Wissenschaftlicher Stand, an den angeknüpft wurde

Eine Darstellung des relevanten Standes der Wissenschaft in Bezug auf das Verbundprojekt findet sich im Schlussbericht des Gesamtprojekts [Sysgo13]. Im Folgenden sind die relevanten Vorarbeiten in Bezug auf das Teilprojekt des Fraunhofer IESE dargestellt.

Das Teilvorhaben fußte auf der Forschung im Bereich zertifizierbarer Separierungskernarchitekturen auf und knüpfte an Vorarbeiten des Fraunhofer IESE und Dritter zur Sicherheitsanforderungsspezifikation und zur Sicherheitsevaluation an. Hinsichtlich der verwendeten Spezifikationsformate wurden die Formalismen der Common Criteria ([CC12], siehe Abschnitt 3.2) verwendet, um eine Standardkonformität der Ergebnisse zu gewährleisten.

3.1 Separierungskerne

In den letzten Jahren haben sich Separierungskerne zunehmend durchgesetzt, um auf einer gemeinsamen Hardware-Plattform verschiedene Anwendungen möglichst wechselwirkungsfrei auszuführen. Vor allem (aber nicht nur) unter Sicherheitsgesichtspunkten ist es vorteilhaft, jeder Anwendung eine eigene, von anderen Anwendungen und vom Betriebssystem strikt abgeschottete logische Partition zuzuordnen, die in keinerlei ungeplante Wechselwirkungen mit anderen Partitionen treten kann.

Ein entsprechender Ansatz im Bereich der Avionik ist *Integrated Modular Avionics* (IMA). Hierbei geht es vor allem darum, bei der Realisierung der immer umfangreicheren Steuerungssoftware Steuergeräte einzusparen, indem man mehrere Software-Steuerungen auf einem gemeinsamen physischen Rechner ausführt. Eine kritische Randbedingung ist dabei die Funktionssicherheit (Safety) des Flugzeugs. Das bedeutet konkret, dass ein Fehler in einer Steuerungsfunktion möglichst keine Auswirkungen auf andere, unabhängige Funktionen haben darf. Bei IMA ist der Einsatz eines Separierungskerns somit ursprünglich vor allem durch Safety-Erwägungen motiviert; erst in neuerer Zeit geraten auch Datensicherheitsgesichtspunkte in das Blickfeld, weil Flugzeug-IT immer stärker mit der Außenwelt vernetzt ist und damit anfälliger für äußere Manipulationen wird.

Eine Entsprechung im Bereich der militärischen Geheimhaltung ist das Konzept der *Multiple Independent Levels of Security* (MILS), einer hochvertrauenswürdigen Architektur für die Trennung und Kontrolle von Informationsflüssen, insbesondere solchen, die als geheimhaltungsbedürftig eingestuft (»classified«) sind [Rus81, AHO+06]. Der MILS-Ansatz zielt auf modulare Systeme aus gegeneinander abgeschotteten Komponenten, was eine nachweislich korrekte Durch-

setzung von Sicherheitsrichtlinien (Security Policies) deutlich vereinfacht: Im Mittelpunkt steht dabei die grundlegende Separierungseigenschaft der »Non-bypassability« vorgegebener, streng überwachter Kommunikationswege, die eine Beweisführung bei der Security-Zertifizierung erheblich vereinfacht oder überhaupt erst möglich macht.

Insgesamt hat sich erwiesen, wie nützlich Separierungskerne sowohl in Bezug auf Safety als auch auf Security für den Entwurf nachweislich sicherer Softwaresysteme sind [AHO+06]. Verschiedene Anbieter haben daher MILS-taugliche Separierungskerne am Markt, darunter zum Beispiel Green Hills Software, Wind River Systems sowie SYSGO [Sysgo12], einer der Projektpartner in diesem Teilvorhaben.

3.2 Common Criteria for IT Security Evaluation

Die *Common Criteria for IT Security Evaluation* (CC) sind eine Norm für die Bewertung und Zertifizierung von IT-Sicherheit. Die CC werden von zahlreichen Staaten gemäß dem *Common Criteria Recognition Arrangement* (CCRA) international anerkannt. Sie sind derzeit in der Fassung von 2008/2009 unter der Bezeichnung ISO/IEC 15408 standardisiert. Zuletzt hat das CCRA Management Committee im September 2012 die neueste Fassung vorgelegt: CC Version 3.1 Revision 4 [CC12].

Im Bereich der Security ist eine Produktzertifizierung nach CC ein anerkanntes Gütekriterium. Zahlreiche sicherheitsrelevante IT-Produkte, zum Beispiel Betriebssysteme, Firewalls, Smartcards und Smartcard-Lesegeräte, sind gemäß CC-konformen Schutzprofilen zertifiziert. Eine Zertifizierung ist nach unterschiedlichen Vertrauenswürdigkeitsgraden möglich, den sogenannten *Evaluation Assurance Levels* (EAL1 bis EAL7). Dabei werden nationale Zertifizierungen auf den niedrigeren Stufen (EAL1–4) gemäß CCRA international anerkannt; höhere Vertrauenswürdigkeitsanforderungen (EAL5–7) erfordern hingegen ein gesondertes Zertifizierungsverfahren in jedem Bestimmungsland.

Ein wesentliches Hemmnis bei der Sicherheitszertifizierung nach CC ist derzeit der erforderliche enorme Evaluationsaufwand [Kal12]. Für komplexere Untersuchungsgegenstände skalieren die existierenden Methoden nur schlecht, und die erforderlichen Zertifizierungsaufwände belaufen sich auf mehrere Personenjahre [HMK12]. Neben der starken Interpretationsbedürftigkeit vieler CC-Klauseln [KMP+11] wird vor allem der Mangel an Konzepten beklagt, um Sicherheitsanalysen geeignet in überschaubare Teilprobleme zu zerlegen, die sich unabhängig voneinander bearbeiten lassen und deren Teilergebnisse sich systematisch zu dem gesuchten Gesamtergebnis zusammenfügen [MBA12].

Im Rahmen des SeSaM-Projekts sollte beispielhaft für Separierungsschicht und eine darauf aufsetzende Anwendung untersucht werden, wie eine modulare Zertifizierung durchgeführt werden kann. Solche »divide et impera«-Strategien sind der Schlüssel, um mit der wachsenden Komplexität moderner Softwaresys-

teme Schritt halten zu können. Ein modularer Evaluationsansatz ermöglicht es zum Beispiel, auf vorhandene Sicherheitszertifikate eines Zulieferers zurückzugreifen und die Analyse des integrierten Systems weitgehend auf Integrationsaspekte zu beschränken. Ein wichtiges Ziel des Teilvorhabens bestand darin auszuloten, wie sich Security-Nachweise und -Argumentationsketten modular zusammenfügen lassen, um daraus global gültige Sicherheitsgarantien abzuleiten.

3.3 Schutzprofil-Spezifikation

Eines der Ziele des Teilprojekts war die Erstellung einer Schutzprofil-Skizze für Separationskerne. Es gibt bereits verschiedene ähnliche Schutzprofile (Protection Profiles, PP), auf deren Vorarbeiten im Projekt zurückgegriffen werden konnte, darunter die folgenden:

- High Robustness Separation Kernel (SKPP, U.S. Information Assurance Directorate, 2007–2011):
  Dieses Schutzprofil basiert noch auf der älteren CC-Version 2.3, entspricht also nicht mehr aktuellen Anforderungen. Das Schutzprofil ist monolithisch und nutzt keinen kompositionalen Evaluierungsansatz. Es zielt allerding auf sehr hohe Vertrauenswürdigkeit, in etwa vergleichbar mit EAL6+.
- High Assurance Separation Kernel (HASK-PP, Sirrix & BSI, 2008):
  Im Mittelpunkt steht hier ein Konzept, um den Vertrauenswürdigkeitsstatus externer Systemkomponenten aus der Ferne verlässlich zu bestimmen und deren Integrität und Authentizität jederzeit nachweisen zu können. Die angestrebte Vertrauenswürdigkeit ist EAL5.
- OSPP und OSPP Extended Package – Virtualisierung (BSI, 2010):
  Dieses Schutzprofil und sein Erweiterungspaket beschreiben zusammen die Anforderungen an ein sicheres universelles Betriebssystem, in dem Subjekte (ausschließlich) über wohldefinierte Kommunikationskanäle miteinander kommunizieren, und Ergänzungen für das Einrichten sicherer Compartments.
  Die angestrebte Vertrauenswürdigkeit ist EAL4+
- CCOPP-OS (Hewlett-Packard, 2008):
  Dieses Schutzprofil ist auf Hewlett-Packards Unix-Implementierung gemünzt und zielt vor allem auf mittleren Schutz gegen gewöhnliche Manipulationsversuche nichtprivilegierter Nutzer, nicht jedoch auf Schutz vor anspruchsvollen Angriffen oder Missbrauch von höheren Nutzerprivilegien.
  Die angestrebte Vertrauenswürdigkeit ist EAL4.

Verglichen mit der im Teilprojekt zu entwickelnden Schutzprofil-Skizze haben die oben genannten Profile, mit Ausnahme von SKPP [IAD07], thematisch eine etwas andere Ausrichtung. Immerhin lieferten sie Anregungen, wie die einschlägigen Bedrohungen, Richtlinien, Sicherheitsannahmen und Schutzziele geeignet dargestellt werden können.

SKPP war den Zielsetzungen des Teilvorhabens am nächsten, beruht jedoch auf einer inzwischen veralteten Version der Common Criteria. Zudem wurde das Profil im Herbst 2011 von den amerikanischen Behörden offiziell zurückgezogen und hat damit seine Gültigkeit verloren (siehe dazu auch Abschnitt 4.5).

3.4 Kompositionale Security-Evaluation

An Ansätzen für eine modulare, inkrementelle Sicherheitsbewertung haben sowohl die Industrie als auch die Forschung ein großes Interesse.

Ansätze im Rahmen der Common Criteria

Die komponentenweise, zusammengesetzte (»kompositionale«) Zertifizierung von IT-Produkten und Software-Systemen ist in der industriellen Anwendung bislang wenig verbreitet. Demgemäß gibt es damit auch nur wenig Erfahrung. Derzeit existieren nur zwei etablierte kompositionale Evaluierungsansätze, die mit dem CC-Zertifizierungsstandard verträglich sind.

Zum einen enthalten die Common Criteria die sogenannten »Component Assurance Packages« (CAP, vgl. [CC12] Part 3, Section 9) sowie die speziell dafür vorgesehenen Klasse »Composition« (Class ACO, vgl. [CC12] Part 3, Section 17) von Nachweispflichten (Security Assurance Requirements, SAR), die bei der kompositionalen Evaluierung zusätzlich zu den üblichen Nachweispflichten zu erfüllen sind. Prinzipiell ermöglicht der CAP-basierte Ansatz die kompositionale Evaluierung beliebig zusammengesetzter Systeme bis zu einem mittleren Vertrauenswürdigkeitsstufe (vergleichbar EAL4), deren Komponenten nicht notwendigerweise hierarchisch gegliedert sein müssen. CAP-Zertifizierungen sind bisher aber nicht gebräuchlich: Eine der wenigen bekannt gewordenen CAP-Anwendungen wird in [Win10] diskutiert.

Als Alternative propagiert das Common Criteria Development Board (CCDB) die »Composite Evaluation Methodology for Smart Cards and similar devices« [CCDB07]. Dieser Ansatz ist speziell auf die Zertifizierung von Smartcard-basierter Software zugeschnitten und ermöglicht prinzipiell auch Zertifizierungen auf hohen und höchsten Vertrauenswürdigkeitsstufen. Allerdings setzt die Methode einen streng hierarchisch strukturierten Untersuchungsgegenstand voraus: eine Hardware-Plattform mit darauf ablaufender Anwendung. Dies beschränkt die Übertragbarkeit der Methode auf andere Anwendungsfelder. Daher ist auch der CCDB-Ansatz wenig gebräuchlich.

Forschungsansätze

Im Allgemeinen bleiben Sicherheitseigenschaften bei Komposition oder Dekomposition sicherer Systeme *nicht* erhalten: Universelle, sicherheitserhaltende Transformationen dieser Art gibt es nicht, wie man anhand einfacher Beispiele zeigen kann. Forschungsseitig kann das Ziel deshalb nur darin bestehen, spezi-

elle Sicherheitseigenschaften anzugeben, für die (unter gegebenen Randbedingungen) sicherheitserhaltende Transformationen möglich sind.

Datta et al. Beschreiben einen solchen Ansatz [DFG+11], basierend auf einer kompositionalen Theorie für funktionale Korrektheit. Dazu modellieren sie Sicherheitsmerkmale als Eigenschaften über Ereignisfolgen (Event Traces), die in Temporallogik spezifiziert sind. Ausgehend von nachweislich komponierbaren lokalen Eigenschaften leiten sie zusammengesetzte Sicherheitseigenschaften ab. Die Beweisführung greift dabei auf bewiesene Invarianten von Schnittstellen und domänenspezifische Grundannahmen zurück. Die so umrissene Klasse von Sicherheitseigenschaften ist nachweislich komponierbar, umfasst allerdings nur eine eingeschränkte Auswahl von Sicherheitsmerkmalen. Lässt sich ein Kompositionsbeweis nach dem von Datta et al. vorgeschlagenen Verfahren nicht vollenden, so liefert dies einen Hinweis, dass man sich die Sicherheitseigenschaften der beteiligten Schnittstellen noch einmal genauer ansehen sollte.

4 Ergebnisse des Teilvorhabens

Eine umfassende Darstellung der Ergebnisse des SeSaM-Gesamtprojekts bietet [Sysgo13]. Das Teilvorhaben des Fraunhofer IESE lieferte folgende Beiträge zum SeSaM-Gesamtvorhaben.

4.1 Systematische Schutzziel-Bestimmung

In den Arbeitspaketen AP1 und AP2 des Verbundvorhabens war Fraunhofer IESE vor allem mit der Erhebung und Dokumentation von Sicherheitsanforderungen an Separierungskerne befasst. Fraunhofer IESE erstellte in Kooperation mit dem DFKI und unter dessen Federführung als akkreditiertem CC-Prüflabor ein generisches Basisschutzprofil für Separierungskerne (Deliverable D.1.1).

AP 1 — Generische Sicherheitsanforderungen an Separierungskerne

In AP1 sichtete Fraunhofer IESE zusammen mit den Verbundpartnern existierende Schutzprofile (vgl. Abschnitt 3.3) und wertete sie hinsichtlich Terminologie und Modellierungsansatz für die Sicherheitsproblemdefinition aus. Auf Basis der vorgeschlagenen Begrifflichkeiten und Modelle wurde eine projektspezifische Basisschutzprofil-Skizze (PP) gemäß aktueller Version der Common Criteria [CC12] formuliert. Dabei war zu berücksichtigen, dass einige der untersuchten Schutzprofile noch auf älteren CC-Versionen fußten. Die betroffenen Vorlagen mussten daher vor der Auswertung in das neue Format der [CC12] übertragen werden.

Ausgehend von den in den herangezogenen Quellen vorgeschlagenen Bedrohungen, Security-Richtlinien und -Annahmen und den daraus resultierenden Sicherheitszielen für den Evaluationsgegenstand und seine Einsatzumgebung entwickelte das Fraunhofer IESE im Projekt eine Kreuzmatrix, die Bedrohungen (Threats), Richtlinien (Policies) und Annahmen (Assumptions) für Separierungskerne mit daraus abgeleiteten Sicherheitszielen (Objectives) für Separierungskerne und deren Einsatzumgebung in Beziehung setzt. Mit Hilfe der Matrix konnte zu jeder Zeit die Abdeckung aller logischen Security-Anforderungen und der Ursprung aller Sicherheitsziele überwacht werden.

Die so gewonnene Liste der Ziele wurde nun in einer zweiten Kreuzmatrix nach dem gleichen Verfahren mit entsprechenden Security Functional Requirements (SFRs) aus [CC12] verknüpft. Die zweite Matrix ermöglicht auf einen Blick die Kontrolle der vollständigen Abdeckung und der ordnungsgemäßen Herleitung aller SFRs, wie in den Common Criteria gefordert.

Es ergab sich schließlich ein Schutzprofil mit funktionalen Sicherheitsanforderungen gemäß Abbildung 1, das vollständig auf den standardisierten, wenn

auch fallspezifisch modifizierten SFRs der [CC12] fußt. Die Vertrauenswürdigkeitsanforderungen (Security Assurance Requirements, SARs) ergeben sich aus dem angestrebten Evaluation Assurance Level (EAL4+); sie sind unmittelbar den Common Criteria [CC12, Part 3] zu entnehmen.

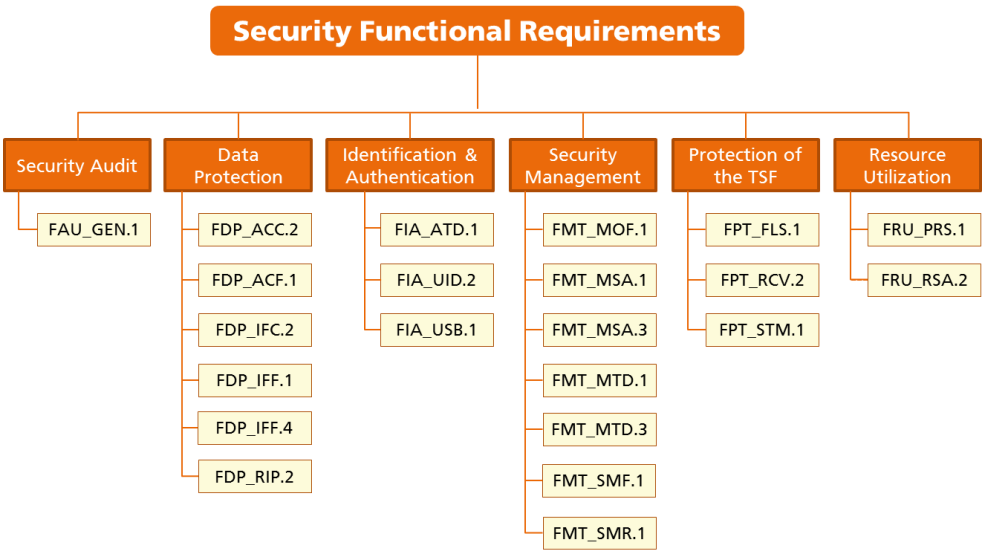


Abbildung 1 Übersicht über identifizierte Schutzziele für Separierungskerne gemäß Common-Criteria-Methodik

Verglichen mit dem Schutzprofil SKPP [IAD07], das eine ähnliche Zielsetzung wie unser Basisschutzprofil verfolgt, ergaben sich eine Reihe wesentlicher Unterschiede:

- SKPP erfordert ausdrücklich eine Begutachtung durch die U.S. National Security Agency. Es enthält somit nationale Bezüge, die im SeSaM-Projekt ausdrücklich vermieden wurden, um eine internationale Anwendbarkeit zu gewährleisten.
- SKPP schließt die Hardware in den Evaluationsgegenstand (TOE) mit ein, während das SeSaM-Schutzprofil Hardware-indifferent formuliert ist und nur wenige, grundlegende Anforderungen an zulässige Hardware-Plattformen macht.
- SKPP erlaubt dynamische Konfigurationsänderungen und externe Benutzerschnittstellen, was das SeSaM-Schutzprofil (mit Blick auf den typischen Anwendungskontext eingebetteter Systeme) ausklammert.
- SKPP erlaubt Seitenkanäle, sofern diese (in Bezug auf den Einsatzzweck) nur unbedeutende Bandbreiten zur verdeckten Übertragung von Informationen bieten. Der Anspruch von SeSaM war es hingegen, logische (d.h., nicht-physikalische) Seitenkanäle vollständig auszuschließen.
- SKPP spezifiziert ausdrücklich kein Evaluation Assurance Level, wobei die Anforderungen des Schutzprofils etwa mit EAL6+ vergleichbar sind (vgl.

[IAD07], Tabelle 6.2). SeSaM zielt auf eine Vertrauenswürdigkeitsstufe im Bereich EAL4+ bis EAL5, stellt also nicht ganz so hohe Nachweisansprüche.

Der SeSaM-Schutzprofilentwurf entspricht somit eher den Anforderungen deutscher und europäischer Systemhersteller und orientiert sich stärker an den Bedürfnissen der zivilen Wirtschaft als sein stärker »militärisch« geprägtes Vorbild SKPP.

AP 2 — Sicherheitsvorgaben für den PikeOS Separierungskern

Parallel zu den Arbeiten am Basisschutzprofil erstellten andere Verbundpartner eine Sicherheitsspezifikation des Evaluierungsgegenstands PikeOS, ein sogenanntes Security Target (ST) in CC-Terminologie.

Während der Arbeiten wurde schnell klar, dass das PP- und das ST-Dokument einen sehr hohen Überdeckungsgrad aufweisen werden. Daher kamen die Kooperationspartner überein, beide Dokumente aus einem gemeinsamen Quelldokument abzuleiten, wobei jeweils die PP- und ST-spezifischen Beschreibungsteile entsprechend gekennzeichnet wurden. Die Integration beider Deliverables in ein gemeinsames Quelldokument erleichterte es erheblich, die Konsistenz der Ergebnisse der beiden Arbeitspakete zu gewährleisten.

Über die im Zuge von AP1 gelieferten Textbausteine zum gemeinschaftlichen Quelldokument hinaus leistete das Fraunhofer IESE in AP2 zum einen Unterstützung bei der Qualitätssicherung des Security Targets. Außerdem übernahm es das Fraunhofer-Institut, die PP- und ST-relevanten Inhalte im integrierten Quelldokument zu ermitteln, entsprechend zu kennzeichnen und mit Verweisen auf die relevanten Klauseln der Common Criteria zu versehen.

Der Beitrag des IESE bestand in diesem Arbeitspaket vor allem in der Aktualisierung und Schärfung der begleitenden Artefakte zu Deliverable D2.1 (»Security Target für den Separierungskern«), insbesondere der Kreuztabellen zur Darstellung der Threats, Policies, Assumptions und daraus abgeleiteten Objectives für PikeOS. Dies war eine wichtige Vorarbeit, um später in AP4 die kompositionale Evaluierung des auf PikeOS basierenden Avionik-Gateways vorantreiben zu können. Die daraus gewonnenen Einsichten flossen in Reviews von Protection Profile (AP1) und Security Target (AP2) ein und führten dort zu kleineren Korrekturen und Ergänzungen.

4.2 Modulare Komposition von Schutzziel-Spezifikationen

Im Arbeitspaket 4 des Verbundvorhabens befasste sich Fraunhofer IESE zusammen mit den Verbundpartnern mit Konzepten und Techniken zur modularen Zertifizierung zusammengesetzter Systeme. Das Arbeitspaket wurde von Fraunhofer IESE geleitet.

Das Ziel des IESE-Teilprojekts war die Entwicklung eines Konzepts für die modulare Evaluierung eines Verbundsystems, bestehend aus dem Separierungskern

PikeOS und einer darauf aufsetzenden Anwendung — im vorliegenden Fall ein Avionik-Sicherheitsgateway. Im Ergebnis wurde gemeinschaftlich eine Spezifikation für eine sogenannte Composite Product Evaluation in ihren Grundzügen erstellt (Deliverable D.4.2), um den kompositionalen Ansatz exemplarisch zu erproben.

Als Vorarbeit für ein kompositionales Evaluierungskonzept führte Fraunhofer IESE zunächst eine vergleichende Bestandsaufnahme zweier konkurrierender Ansätze durch und verglich deren Anforderungen und Aussagekraft. Es handelte sich zum einen um die »Composite Evaluation Methodology for Smart Cards and similar devices« [CCDB07], zum anderen um die »Component Assurance Packages« (CAP) gemäß Common Criteria [CC12, Part 3, Section 9]. Die Analyse wurde in zwei Berichten dokumentiert.

Da sich das Projektkonsortium schließlich dafür entschied, im Projekt den CAP-basierten Ansatz zu verfolgen, nimmt der Bericht zu [CCDB07] auf den Bericht zu CAP Bezug und stellt die Unterschiede und Gemeinsamkeiten besonders heraus. In künftigen Arbeiten außerhalb des SeSaM-Projekts [EMILS13] sollen diese Ergebnisse aufgegriffen werden, um auch das alternative Verfahren zur modularen Evaluierung einer genaueren Erprobung zu unterziehen. Die vorliegende Analyse zu [CCDB07] kann hier zum Ausgangspunkt genommen werden.

Nachdem CAP-C einvernehmlich als kompositionaler Evaluierungsansatz festgelegt war, erarbeiteten IESE und EADS das Grundgerüst für eine CAP-gemäße Security Target (ST) Spezifikation für das Avionik-Gateway. Kernelement dieses ST ist die sogenannte Security Problem Definition, die für eine modulare Evaluierung in zwei Teile zu spalten ist:

- jenen Teil des Problems, der mit den Mechanismen der abgeleiteten Komponente (im Beispiel das Avionik-Gateway) zu lösen ist, sowie
- den verbleibenden Teil des Sicherheitsproblems, der bereits durch die Mechanismen der Basiskomponenten (in unserem Falle der Separierungskern PikeOS) gelöst wird.

Zu diesem Zweck wurde zunächst das Security-Problem gemäß den Empfehlungen des Standards ISO/IEC 15446 matrixbasiert erhoben. Abbildung 2 zeigt das Analysetableau im Überblick, mit dessen Hilfe die zu schützenden Werte (Assets), kritischen Bedrohungen (Threats), Bedrohungsquellen (Threat Agents) und Angriffsvektoren (Adverse Actions) systematisch eruiert wurden.

Die so ermittelten Bedrohungen wurden nun nach dem zuvor festgelegten Konzept in eine Analysematrix gemäß Abbildung 3 übertragen, zusammen mit den geltenden Security-Richtlinien sowie weiteren Grundannahmen, auf denen das technische Konzept des Avionik-Gateways basiert.

Ausgehend von diesem Zwischenschritt wurden nun Sicherheitsziele (Security Objectives) für das Gateway sowie für dessen Einsatzumgebung abgeleitet und

als Spalten in die Matrix übernommen. Letztere, die Umgebungsziele, wurden danach auf entsprechende Sicherheitsziele der Basiskomponente (Separierungskern) abgebildet, wo dies möglich war: Die abbildbaren Ziele bezeichnen nun Sicherheitsgarantien, die sich bereits aus der Evaluierung der Basiskomponente ergeben; der verbleibende, nicht abbildbare Rest stellt Einschränkungen dar, die bei der Verwendung des Gateways zu beachten sind und entweder durch organisatorische oder durch zusätzliche technische Vorkehrungen gewährleistet werden müssen. Für die technisch zu realisierenden Sicherheitsziele des Gateways wurden im Rahmen der ST-Spezifikation entsprechende Security Functional Requirements (SFRs) der Common Criteria konkret zugeordnet.

Threat Agent **Adverse Action**	**Attacker** (external malicious entity)	**Authorized Subject** (non-human)	**Trusted Subject** (non-human)	**Trusted Individual** (external entity)
improper access (interception, disclosure, corruption, deletion, forgery, unauthorized access)	* System Data (unauthorized access[9], manipulation[9]); * Audit Trail (manipulation[9], disclosure[4,9]); * User Data (unauthorized access[9], manipulation[9]); * Client Data [Information flows handled by Security Gateway] (Integrity[9] or confidentiality[4] violations, circumvention of filtering[2,4]); * Processes (unauthorized access[9]) * Physical entities [hardware, cabeling, and power supply] (manipulation[3,9]);	* System Data (unauthorized access[9], manipulation[9]); * Audit Trail (unauthorized access[9], manipulation[9], disclosure[4,9]); * User Data (unauthorized access[9], manipulation[9]); * Processes (unauthorized access[9]) ** Client Data [Information flows handled by Security Gateway] (Integrity[9] or confidentiality[2,4,9] violations);	* System Data (misconfiguration[1,8], manipulation[1,8]); * Audit Trail (disclosure[4], manipulation[8]); * User Data (manipulation[8]);	* System Data (manipulation[7], misconfiguration[7]); * Audit Trail (manipulation[7], disclosure[4]); * User Data (manipulation[7]); * Physical entities (manipulation[7], misconfiguration[7])
improper transfer of access rights (masquerade, elevation of privilege)	* TSF data (elevation of privileges[3]); * User data (elevation of privileges[9]); * Processes (manipulation of process priorities[3,9]);	* TSF data (elevation of privileges[3]); * User data (elevation of privileges[9]); * Processes (manipulation of process priorities[3,9])	* System Data (permission grants to untrusted individuals or subjects[8]); * Audit Trail (permission grants to untrusted or unauthorized individuals or subjects[4]); * User Data (permission grants to unauthorized security domains[8]); * Processes (manipulation of process priorities[3])	* System Data (unwarranted trust in trusted individuals[7], permission grants to untrusted individuals or subjects[7]); * Audit Trail (permission grants to untrusted or unauthorized individuals or subjects[4,7]); * User Data (permission grants to unauthorized security domains[7]); * Processes (manipulation of process priorities[3]) * Physical entities (unwarrented access permissions for external entities[7])
denial of legitimate access (Denial of Service)	* Client Data (interruption of communication[3]) * Processes (priority degradation[3], monopolization of resources or locks[3], interruption of communication[3], unfounded shutdown[3]) * Physical entities (destruction[3,5], deprivation[3,5], manipulation[5,9])	* Client Data (interruption of communication[3]) * Processes (priority degradation[3,9], monopolization of resources or locks[3,9], interruption of communication[3], unfounded shutdown[3,9])	* Client Data (interruption of communication[3,8]) * Processes (priority degradation[3,8], monopolization of resources or locks[3,8], interruption of communication[3,8], unfounded shutdown[3,8])	* Client Data (interruption of communication[3]) * Processes (priority degradation[3], monopolization of resources or locks[3], interruption of communication[3], unfounded shutdown[3], insufficient resource or computing power assignment[3,7]); * Physical entities (destruction[3,5], insufficient hardware redundancy or power supply[5,7]);
non-accountability (repudiation)		* TSF Data (manipulation of account identity[6,9]) * Audit Trail (circumvention[6], disabling[6,9], overflow[6], manipulation[6,9])	* TSF Data (manipulation of account identity[6,8]) * Audit Trail (disabling[6,8], circumvention[6,8], overflow[6,8], manipulation[6,8])	* TSF Data (manipulation of account identity[6]) * Audit Trail (insuffcient recording capacity assignment[5,6], circumvention[6], disabling[6], overflow[6], manipulation[6])
	Assets affected (type of impairment)			

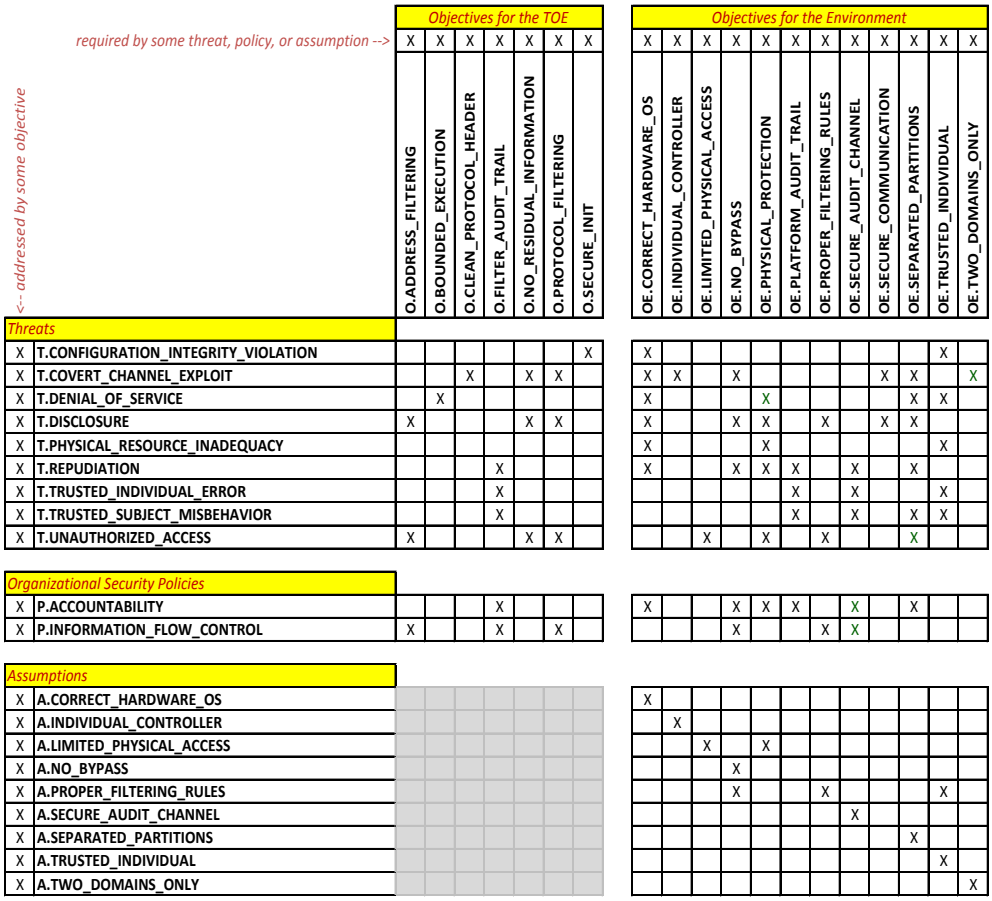
Asset Types (according to ISO TR 15466)		
Information	System Data (TSF Data in particular)	
	User Data	General Data
		Special Data
		Client Data
Processes		
Physical entities		

Threats attributed to the above adverse actions:

1. T.CONFIGURATION_INTEGRITY_VIOLATION
2. T.COVERT_CHANNEL_EXPLOIT
3. T.DENIAL_OF_SERVICE
4. T.DISCLOSURE
5. T.PHYSICAL_RESOURCE_INADEQUACY
6. T.REPUDIATION
7. T.TRUSTED_INDIVIDUAL_ERROR
8. T.TRUSTED_SUBJECT_MISBEHAVIOR
9. T.UNAUTHORIZED_ACCESS

Abbildung 2 Ausschnitt aus der Tableau-basierten Bedrohungsanalyse für das Avionik-Gateway

Aufgrund der Analysen zeichnete sich nun ab, welche Security-Leistungen die abhängige Komponente (Avionik-Gateway) von der Basiskomponente (Separierungskern) und der Einsatzumgebung fordert und welche Leistungen umgekehrt die Basiskomponente für die abhängige Komponente bereitstellt. Daraus ergeben sich die »Beweisverpflichtungen« in Bezug auf die einzelnen Systemkomponenten, die notwendig sind, um insgesamt eine schlüssige kompositionale Evaluierung des Gesamtsystems zu erhalten. Die systematische Auftrennung der Nachweispflichten in unabhängige, aber einander entsprechende Module ist der Kern des in AP4 angestrebten modularen Zertifizierungsverfahrens.



		Objectives for the TOE							Objectives for the Environment											
	required by some threat, policy, or assumption -->	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	<-- addressed by some objective	O.ADDRESS_FILTERING	O.BOUNDED_EXECUTION	O.CLEAN_PROTOCOL_HEADER	O.FILTER_AUDIT_TRAIL	O.NO_RESIDUAL_INFORMATION	O.PROTOCOL_FILTERING	O.SECURE_INIT	OE.CORRECT_HARDWARE_OS	OE.INDIVIDUAL_CONTROLLER	OE.LIMITED_PHYSICAL_ACCESS	OE.NO_BYPASS	OE.PHYSICAL_PROTECTION	OE.PLATFORM_AUDIT_TRAIL	OE.PROPER_FILTERING_RULES	OE.SECURE_AUDIT_CHANNEL	OE.SECURE_COMMUNICATION	OE.SEPARATED_PARTITIONS	OE.TRUSTED_INDIVIDUAL	OE.TWO_DOMAINS_ONLY
Threats																				
X	T.CONFIGURATION_INTEGRITY_VIOLATION							X	X										X	
X	T.COVERT_CHANNEL_EXPLOIT			X		X	X		X	X		X					X	X		X
X	T.DENIAL_OF_SERVICE		X						X				X					X	X	
X	T.DISCLOSURE	X				X	X		X			X	X		X		X	X		
X	T.PHYSICAL_RESOURCE_INADEQUACY								X				X						X	
X	T.REPUDIATION				X				X			X	X	X		X		X		
X	T.TRUSTED_INDIVIDUAL_ERROR				X									X		X			X	
X	T.TRUSTED_SUBJECT_MISBEHAVIOR				X									X		X		X	X	
X	T.UNAUTHORIZED_ACCESS	X				X	X				X		X		X			X		
Organizational Security Policies																				
X	P.ACCOUNTABILITY				X				X			X	X	X		X		X		
X	P.INFORMATION_FLOW_CONTROL	X			X		X					X			X	X				
Assumptions																				
X	A.CORRECT_HARDWARE_OS								X											
X	A.INDIVIDUAL_CONTROLLER									X										
X	A.LIMITED_PHYSICAL_ACCESS										X		X							
X	A.NO_BYPASS											X								
X	A.PROPER_FILTERING_RULES											X			X				X	
X	A.SECURE_AUDIT_CHANNEL															X				
X	A.SEPARATED_PARTITIONS																	X		
X	A.TRUSTED_INDIVIDUAL																		X	
X	A.TWO_DOMAINS_ONLY																			X

Abbildung 3 Modulare Abbildung von Bedrohungen, Richtlinien und Annahmen auf Sicherheitsziele (Ausschnitt)

4.3 Beiträge zum Prä-Evaluationsbericht

In den Arbeitspaketen AP6 des Verbundvorhabens trug das Fraunhofer IESE zum Prä-Evaluationsbericht (Deliverable D.6.1) bei. Da sich aufgrund der kom-

positionalen Evaluierung in Arbeitspaket 4 nur ein geringer Ergänzungsbedarf an der Spezifikation des Separierungskerns ergab, entfiel der überwiegende Beitrag in diesem Arbeitspaket auf Review-Tätigkeiten zur Qualitätssicherung des Deliverables, das federführend von den Projektpartnern DFKI und SYSGO erstellt wurde.

4.4 Gegenüberstellung der Ergebnisse mit den Projektzielen

Systematische Schutzziel-Bestimmung (AP1)

Der im Arbeitspaket 1 eingeschlagene Weg erwies sich als effektiv, um zügig zu einem Basisschutzprofil für den Separierungskern zu gelangen. Diskussionsbedarf entstand vor allem in Bezug auf die Wahl eines passenden Abstraktionsniveaus für die Bedrohungsmodellierung: Wie spezifisch oder wie generisch sollen Bedrohungen definiert werden, um daraus die notwendigen Schutzziele abzuleiten. Zur Beantwortung dieser Frage erwies es sich als hilfreich, sich an anderen, ähnlichen Schutzprofilen zu orientieren. Am Ende kamen die Verbundpartner überein, Bedrohungen — d.h. Tripel der Form {Threat Agent, Asset, Adverse Action} — eher allgemeiner zu formulieren.

Wertvolle Anregungen für das allgemeine Schutzprofil lieferte im Kontext des Projekts die konkrete Schutzziel-Spezifikation für den Separierungskern. Obwohl Fraunhofer IESE nicht unmittelbar mit dieser Aufgabe befasst war, lieferte der enge Austausch zwischen den Arbeitspaketen AP1 und AP2 wertvolle Anregungen für generalisierte Sicherheitsanforderungen. Umgekehrt schärfte das Basisschutzprofil den Blick für die konkrete Schutzziel-Spezifikation für den PikeOS-Separierungskern.

Modulare Komposition von Schutzziel-Spezifikationen (AP4)

Der Schlüssel für einen erfolgreichen kompositionalen Evaluierungsansatz ist die saubere Zuordnung der Schutzziele zur Basiskomponte, zur abhängigen Komponente oder zur gemeinsamen Einsatzumgebung. Hier erwies es sich als unabdingbar, zunächst eine solide Schutzziel-Spezifikation für die Basiskomponente zu erstellen, um eine klare Abgrenzung der Verantwortlichkeiten zu ermöglichen. Die matrixbasierte Analyse half bei der Rückverfolgung und Vollständigkeitsüberwachung der Sicherheitsanforderungen.

Im vorliegenden Fall erwies sich der Separierungskern als ein besonders anspruchsvoller Kandidat für einen modularen Evaluierungsansatz, denn seine Schnittstelle entspricht nicht den üblichen Erwartungen der Common Criteria an eine Basiskomponente im Sinne der Component Assurance Packages (vgl. Abbildung 4): Der CAP-Ansatz der Common Criteria geht davon aus, dass die Sicherheitsfunktionen der abhängigen Komponente (Target of Evaluation Security Functionality, TSF) auf eine wohldefinierte Menge von TSF und Nicht-TSF der Basiskomponente zurückgreifen, so dass sich die Sicherheitsbetrach-

tung im Wesentlichen auf diese expliziten Schnittstellenaufrufe eingrenzen lässt.

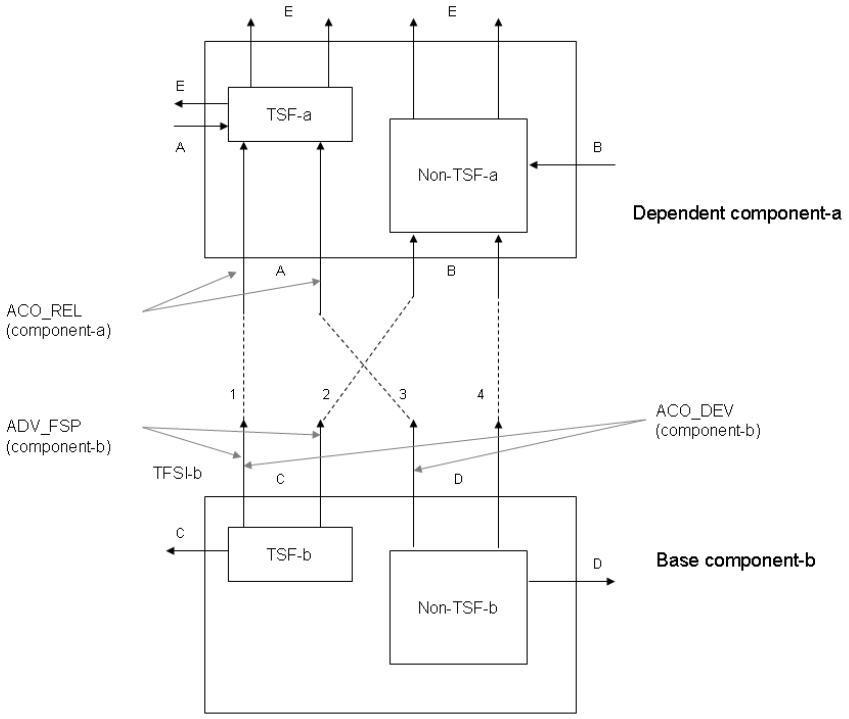


Abbildung 4 Schnittstellenmodell für Komposit-Systeme gemäß [CC12, Part 3]

Ein Separierungskern als Basiskomponente bietet der abhängigen Komponente jedoch als zentrale Sicherheitsfunktionalität keine solche explizite Schnittstelle; seine wesentliche TSF besteht darin, die Partition(en) der Anwendung gegen äußere Einflüsse abzuschotten. Diese Abschottungsfunktionalität lässt sich jedoch nicht an einzelnen Funktionsaufrufen festmachen, sondern bezieht sich auf jegliche Aktivität der abhängigen Anwendung—wenn man so will, auf jeden Maschinenbefehl des Anwendungscodes.

Aufgrund dieser Besonderheit in der Beziehung zwischen Basiskomponente und abhängiger Komponente musste die Standardvorgehensweise des CAP-Ansatzes im vorliegenden Fall modifiziert werden. Die Verbundpartner DFKI und SYSGO nahmen es dazu auf sich, die informationsflussrelevante Wirkung der Separierungskern-Operationen formal zu modellieren (vgl. [Sysgo13], Abschnitt 2.1.3 »Formale Methoden«). Das formale Modell schafft die Voraussetzungen, um die sicherheitserhaltenden Eigenschaften der Komponentenkomposition (mittels geeigneter Verifikationswerkzeuge) formal zu beweisen. Dieser Weg wurde im Verbundvorhaben erfolgreich beschritten, sorgte im Arbeitspaket 4 jedoch für zuvor unerwartete konzeptionelle Schwierigkeiten, die überwunden werden mussten.

Für die Praxis bedeutet dies, dass die kompositionale Zertifizierung einer Separierungskern-basierten Anwendung ohne ein entsprechendes formales Modell für den Separierungskern mit den bisher anerkannten Verfahren kaum durchführbar ist. Der in den Common Criteria propagierte kompositionale Evaluierungsansatz ist in diesem Anwendungsbereich somit nur eingeschränkt praktikabel.

4.5 Bekanntgewordene Ergebnisse Dritter auf dem Gebiet

Während der Projektlaufzeit gab es folgende Entwicklungen außerhalb des Projekts, die für die Zielsetzungen des Teilvorhabens relevant waren. Weitere Entwicklungen, die für das Verbundprojekt insgesamt relevant waren, sind im Gesamtschlussbericht [Sysgo13] im Abschnitt 2.3 beschrieben.

Abkündigung des SKPP

Im Mai 2011 gab die U.S. National Information Assurance Partnership (NIAP) die Abkündigung des »U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness« (SKPP) bekannt, mit Wirkung zum 1. September 2011. Da das SKPP für SeSaM einen wichtigen Referenzpunkt im Bereich der Schutzprofile für hochsichere Separierungskerne darstellt, ist dies ein bemerkenswerter Schritt für die internationale High Assurance Community.

Zur Begründung für die Abkündigung führt NIAP vor allem folgende Punkte ins Feld:

- NIAP will sich künftig vor allem den niedrigeren Evaluation Assurance Levels unterhalb von EAL5 widmen, die für kommerzielle Standardprodukte in der Regel angemessen sind. SKPP war jedoch eher im Bereich EAL6+ angesiedelt und adressierte insbesondere sicherheitsrelevante Militär- und Regierungssysteme der USA.
- Der Aufwand zur Prüfung und Aufrechterhaltung sehr hoher Assurance Levels und die notwendige Pflege entsprechender generischer Schutzprofile werden von NIAP als zu aufwändig eingestuft. Für solch hohen Schutzbedarf will sich die U.S. National Security Agency (NSA) gezielt mit den individuellen Systemen befassen und sich den Aufwand sparen, unspezifische Schutzprofil-Eigenschaften zu formulieren oder zu evaluieren.
- Im Hochsicherheitsbereich wird die NSA künftig den Schwerpunkt auf die Prüfung von Assurance-Argumenten und deren Beweisführung legen, nicht aber auf die Erfüllung von Security-Anforderungen.

Die Arbeiten in SeSaM begegnen diesen Argumenten, indem sie von vornherein eine niedere EAL-Stufe als SKPP anvisieren und indem der Untersuchungsgegenstand enger gefasst wird. So vermeidet SeSaM etwa, die Hardware-Plattform mit in den Evaluationsgegenstand einzubeziehen. Darüber hinaus lag der Schwerpunkt des Vorhabens eher in der Methodenentwicklung für Evaluie-

rung konkreter Systeme als auf der Bereitstellung eines universellen Schutzprofils. Demgemäß wurde im Arbeitspaket 1 des Verbundprojekts das Schutzprofil nur als exemplarische Skizze erstellt, und zwar zusammen mit der konkreten Spezifikation des Evaluierungsgegenstands in einem gemeinsamen Dokument.

Einschränkung des Vorschlagsrechts für Schutzprofile

Die CCRA-Mitglieder haben sich offenbar darauf verständigt, dass — anders als in der Vergangenheit — Schutzprofile (Protection Profiles, PPs) künftig nicht mehr von einzelnen Bewerbern vorgeschlagen werden sollen, sondern nur noch von maßgeblichen Industriekonsortien. Damit verlieren die SeSaM-Arbeiten an der Protection-Profile-Skizze an unmittelbarer Außenwirkung und dienten vor allem projektintern der Vorbereitung der Spezifikation des Evaluierungsgegenstands (Security Target, ST). Somit hat sich die Entscheidung des SeSaM-Konsortiums, PP und ST in einem gemeinsamen Quelldokument zu pflegen, nachträglich als vorteilhaft erwiesen, weil damit einerseits die ST-Pflege durch unmittelbaren PP-Bezug zügiger voranschreiten konnte und andererseits durch Wiederverwendung PP-Aufwände eingespart wurden.

Ursprünglich hatten die Verbundpartner einmal ins Auge gefasst, nach Abschluss des Projekts mit der erarbeiteten PP-Skizze an das Bundesamt für Sicherheit in der Informationstechnik (BSI) heranzutreten und gegebenenfalls eine förmliche Anerkennung des Schutzprofils anzustreben, etwa nach dem Vorbild von HASK-PP [KKS+08]. Dieser Plan wurde aufgrund der aktuellen Beschlussfassung der CCRA-Mitglieder fallengelassen.

5 Verwertung der Projektergebnisse

Die Ergebnisse des SeSaM-Verbundvorhabens haben in mehrfacher Hinsicht Verwertung gefunden. Einen Gesamtüberblick über die Verwertbarkeit und Anschlussfähigkeit der Verbundergebnisse liefern der Gesamtschlussbericht und der Gesamterfolgskontrollbericht des Konsortialführers [Sysgo13, Sysgo13b]. Nachfolgend seien die wichtigsten verwertbaren Ergebnisse des IESE-Teilvorhabens genannt.

5.1 Beitrag zu den förderpolitischen Zielen

Das Teilvorhaben wurde seitens des BMBF im Rahmen des Arbeitsprogramms »IT-Sicherheitsforschung« gefördert. Dieses Arbeitsprogramm adressiert ausdrücklich den Aspekt »Eingebaute Sicherheit« als ein wichtiges Entwicklungsziel künftiger Informations- und Kommunikationstechnologie. Als eine der möglichen Herangehensweisen wird unter anderen »die Nutzung von Trusted Computing (oder ähnlichen Funktionalitäten) bei Betriebssystemen und anderer systemnaher Software« genannt.

Das SeSaM-Projekt zielte auf einen solchen Ansatz: die Nutzung einer hochsicheren, zertifizierten Virtualisierungsschicht (eines sogenannten Separierungskerns) als vertrauenswürdige Separierungslösung für die unabhängige Ausführung sicherheitskritischer Software-Module. Dabei leiten die virtualisiert ausgeführten Anwendungsprogramme ihren Sicherheitsanspruch von nachgewiesenen Safety- und Security-Eigenschaften der Ausführungsplattform ab. Der Separierungskern liefert die erforderlichen Sicherheitsgarantien, insbesondere in Bezug auf Informationsflusskontrolle und strikte Ressourcentrennung, auf deren Basis Trusted Computing realisiert werden kann.

Um das Fernziel uneingeschränkt vertrauenswürdiger Separierungslösungen mit wirtschaftlich vertretbarem Aufwand zu erreichen, fehlte es bisher jedoch an Grundlagen im Bereich der Security-Zertifizierung von Separierungsschichten. Im SeSaM-Projekt wurden gemäß den förderpolitischen Zielen des Arbeitsprogramms wichtige »Grundlagen und Konzepte für den korrekten, vertraulichen und sicheren Betrieb von IT« erarbeitet. Dies soll künftig dem Einsatz solcher Separierungskerne in sicherheitskritischen zertifizierten Anwendungen den Weg ebnen, etwa im Bereich der Avionik oder automobiler Steuergeräte.

5.2 Wissenschaftlich-technische Erfolgsaussichten nach Projektende

Das Fraunhofer Institut für Experimentelles Software Engineering (IESE) versteht sich als Vermittler zwischen Forschung und industrieller Praxis. Es berät vor allem auch kleine und mittlere Unternehmen in Sicherheitsfragen. Das Teilvorha-

ben trägt zur Stärkung der Methoden- und Beratungskompetenzen auf dem Gebiet der integrierten Safety und Security bei.

Das Projekt SeSaM versetzt das IESE in die Lage, seine Projektpartner in Bezug auf standardkonforme, sichere eingebettete Plattformarchitekturen kompetenter zu beraten. Mit den entwickelten Spezifikationen für sichere Mikrokern-Virtualisierungslösungen kann das Institut seinen Auftraggebern kurzfristig konkrete Lösungsbausteine anbieten, insbesondere in attraktiven Zukunftsmärkten wie Medizintechnik, Assistenzsystemen (z. B. Ambient Assisted Living) oder Automotive Software Engineering, bei denen es gleichermaßen auf Funktions- und Informationssicherheit ankommt.

Konzepte, wie man einerseits Umwelt und Nutzer des Systems vor Systemversagen schützen (Safety) und zugleich das System gegen eine potentiell feindliche Umwelt verteidigen kann (Security), werden derzeit verstärkt nachgefragt, etwa im Bereich der Nutzfahrzeuge, einem der Geschäftsfelder des Fraunhofer IESE. Eine nachweislich sichere Separierungsschicht dient sowohl der Security als auch der Safety. Kompetenzen auf diesem Gebiet kommen dem Institut damit unmittelbar zugute. Durch die wissenschaftliche Verwertung des Teilprojekts ergeben sich für Fraunhofer IESE voraussichtlich neue Kooperationsmöglichkeiten mit Industriekunden.

Die im Projekt angewendeten systematischen Methoden zur Bedrohungsanalyse (Threat Analysis) und zur Erhebung der Sicherheitsziele (Security Problem Definition) konnten bereits in ersten Kundenprojekten des Fraunhofer IESE nutzbringend weiterverwendet werden, sowohl in der Nutzfahrzeuge-Domäne für eingebettete Software als auch im Bereich von Informationssystemen zur Analyse von geplanten Web Services. Wir gehen davon aus, dass diese methodischen Grundlagen allgemein als Techniken des Secure Software Engineering etabliert werden können.

Abgesehen von dem konkreten Ziel, einen Security-Nachweis für Separierungslösungen zu konzipieren, berührt das Teilvorhaben ein sehr viel grundlegenderes Sicherheitsproblem: Die Frage der Modularität von Security-Eigenschaften. Es ist bekannt, dass Security — anders als viele andere Qualitätsmerkmale von Software — im Allgemeinen weder komponierbar ist, noch invariant bezüglich Verfeinerung [SP07, pp. 132–133]. Das bedeutet, dass sich die nachweisliche Sicherheit eines Grobkonzepts (Entwurf) nicht unbedingt auf das Feinkonzept (Implementierung) überträgt und dass umgekehrt durch die Integration mehrerer nachweislich sicherer Komponenten nicht unbedingt ein sicheres Gesamtsystem entsteht.

Im Teilvorhaben wurde exemplarisch durchexerziert, wie sich Sicherheitseigenschaften dennoch auseinanderdividieren und bei Bedarf wieder zu einer Composite Evaluation zusammenfügen lassen. Auch wenn dabei einige prinzipielle Schwierigkeiten und Beschränkungen deutlich wurden, hat die im Projekt konzipierte Vorgehensweise Modellcharakter für ähnliche Fragestellungen im Um-

feld von Datenfluss-, Zugriffs- oder Nutzungskontrolle, einem der aktuellen Forschungsschwerpunkte des Fraunhofer IESE.

5.3 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Modulare, verteilte Software-Systeme, wie etwa Cloud-Computing-Anwendungen oder mobile Geschäftsanwendungen, sind aktuelle Megatrends in der Informationstechnik. Für solche Systeme, die zunehmend auch in kritischen Anwendungsbereichen eingesetzt werden, sind modulare Sicherheitsbetrachtungen unverzichtbar, um den Aufwand für Sicherheitsnachweise in Grenzen zu halten.

Fraunhofer IESE hat in der Folge des SeSaM-Teilvorhabens mehrere Forschungsprojekte akquiriert, die sich unter anderem mit der Qualitätssicherung solcher Architekturen und Nutzungskontroll-Aspekten in solchen Systemen befassen. In diesem Kontext werden Konzepte und Techniken zur modularen Sicherheitsbetrachtung weiterverfolgt, um für die künftigen Anforderungen praktikable Sicherheitslösungen bereitzustellen. Auch die Verbundpartner nutzen die SeSaM-Ergebnisse in weiterführenden Forschungs- und Entwicklungsvorhaben.

SINNODIUM

Im BMBF-geförderten Verbundprojekt SINNODIUM [SINNO13] untersucht Fraunhofer IESE zusammen mit anderen Forschungspartnern Komponenten für sichere und fehlertolerante Unternehmenssoftware. Einer der ins Auge gefassten Mechanismen sind sogenannte Trusted Virtual Domains, die zusammengehörige Informationsflüsse kapseln und Domain-überschreitenden Informationsaustausch nur über eigens konfigurierte Kommunikationskanäle erlauben, wobei explizit formulierte Sicherheitsrichtlinien (Security Policies) definieren, welchen Einschränkungen solche Inter-Domain-Kommunikation unterworfen ist. Um die Sicherheit so strukturierter Unternehmensanwendungen zu beurteilen, kommen modulare Evaluierungstechniken zum Tragen, wie sie in SeSaM entwickelt wurden.

SECCRIT

Im europäischen Forschungsprojekt SECCRIT [SCRIT13] erforscht Fraunhofer IESE benutzerfreundliche, kontext-sensitive Sicherheitsrichtlinien für Cloud-Computing-Plattformen. Auch hier sind abgeschottete, virtuelle Maschinen [RG05] ein wesentliches Mittel, um in einer Cloud-Umgebungen verschiedene Anwendungen unterschiedlicher Kunden wechselwirkungsfrei parallel zu betreiben und flexibel auf wechselnde Cloud-Ressourcen umzuverteilen. Dabei ist unklar, wie die mit dem Anwender vereinbarten Sicherheitsrestriktionen zuverlässig und nachweisbar durchgesetzt werden können, etwa vorgegebene Orts-, Zeit- oder Kollokationsbeschränkungen. Ein vollständiger Sicherheitsnachweis erfordert neben einer Betrachtung der dynamisch durchgesetzten Policy-

Restriktionen auch einen Nachweis, dass die auf Separationskernen basierenden Plattformen überhaupt spezifikationsgemäß arbeiten und eine korrekte Partitionierung der Anwendungs- und Betriebssystemsoftware vornehmen. Um dies mit vertretbarem Aufwand nachzuweisen, kann wieder auf modulare Evaluierungstechniken zurückgegriffen werden, die dazu auf den Cloud-Kontext angepasst werden müssen.

EURO-MILS

Die SeSaM-Partner SYSGO, EADS und DFKI werden die in SeSaM entwickelten Methoden und einige der dort erarbeiteten Artefakte im Verbundprojekt EURO-MILS [EMILS13] weiterverwenden. Das Projekt wird die Verwendung von MILS-Systemen zur Verbesserung der Avionik-Sicherheit untersuchen und nutzt dazu unter anderem auch die SeSaM-Analyseverfahren. Im Automotive- und Avionik-Umfeld gibt es einen wachsenden Markt für nachweisbare sichere Steuergeräte im Sinne der Informationssicherheit (Security), den der Wirtschaftspartner SYSGO, der auf dem Gebiet der Funktionssicherheit (Safety) schon sehr gut etabliert ist, durch seinen Kompetenzaufbau im MILS-Bereich in den nächsten Jahren verstärkt bedienen will (vgl. dazu die Verwertungspläne in [Sysgo13], Abschnitt 2.2).

5.4 Erfindungen und Schutzrechtsanmeldungen

Im SeSaM-Verbundvorhaben wurden methodische Grundlagen erarbeitet, aber keine Produkttechnologien entwickelt. Daher erfolgten im Kontext des Projekts keine Schutzrechtsanmeldungen, und es mussten auch keine Schutzrechte Dritter in Anspruch genommen werden. Die Verbundpartner sehen die Ergebnisse aber auch nicht durch Anmeldungen von dritter Seite gefährdet.

5.5 Veröffentlichung der SeSaM-Projektergebnisse

Die wichtigsten Informationen zum SeSaM-Verbundvorhaben werden vom Konsortialführer SYSGO im Internet auf einer gesonderten Projektseite bereitgestellt [SeSaM11]. Auf der Internet-Seite des Projekts sind unter anderem auch die aus dem Projekt hervorgegangenen Veröffentlichungen der Projektergebnisse gelistet, darunter folgende Publikationen und Konferenzbeiträge mit Beteiligung des Fraunhofer IESE (in chronologischer Reihenfolge):

[BLM+12] H. Blasum, B. Langenstein, K. Müller, A. Nonnengart, M. Paulitsch, R. Schwarz, W. Stephan, S. Tverdyshev: *Safe and Secure Virtualization: From a DO-178B Certified Separation Kernel to Common Criteria Security Certification.* Presentation, Avionics Europe, Munich, Germany, March 2012

[STB+12] W. Stephan, S. Tverdyshev, H. Blasum, B. Langenstein, K. Müller, A. Nonnengart, M. Paulitsch, R. Schwarz: *CC Compositional*

Certification for MILS Virtualization Platforms. In: Proceedings International Common Criteria Conference (ICCC), Paris, France, September 2012

[MPS+12] K. Müller, M. Paulitsch, R. Schwarz, S. Tverdyshev, H. Blasum: *MILS-Based Information Flow Control in the Avionic Domain: A Case Study on Compositional Architecture and Verification.* In: Proceedings 31st Digital Avionics Systems Conference (DASC), Williamsburg, VA, pp. 7B1-1 – 7B1-13, October 2012. Digital Object Identifier: 10.1109/DASC.2012.6382411 *(von der DASC mit »Best of Session« ausgezeichnet)*

[BLM+13] H- Blasum, B. Langenstein, K. Müller, A. Nonnengart, M. Paulitsch, R. Schwarz, W. Stephan, and S. Tverdyshev: *MILS-related Information Flow Control in the Avionic Domain: Software Architectures and Verification.* Presentation, Avionics Europe, Munich, Germany, February 2013

Eine vollständige Liste der im SeSaM-Kontext entstandenen Publikationen sowie von Pressemitteilungen zum Projekt ist dem Gesamtschlussbericht des Konsortialführers [Sysgo13] zu entnehmen.

Quellenverzeichnis

[AHO+06] J. Alves-Foss, W.S. Harrison, P. Oman, and C. Taylor: *The MILS Architecture for High Assurance Embedded Systems.* International Journal of Embedded Systems 2(3), pp. 239–247, 2006

[BLM+12] H. Blasum, B. Langenstein, K. Müller, A. Nonnengart, M. Paulitsch, R. Schwarz, W. Stephan, S. Tverdyshev: *Safe and Secure Virtualization: From a DO-178B Certified Separation Kernel to Common Criteria Security Certification.* Avionics Europe, Munich, Germany, March 2012

[BLM+13] H. Blasum, B. Langenstein, K. Müller, A. Nonnengart, M. Paulitsch, R. Schwarz, W. Stephan, and S. Tverdyshev: *MILS-related Information Flow Control in the Avionic Domain: Software Architectures and Verification.* Presentation, Avionics Europe, Munich, Germany, February 2013

[CC] *The Common Criteria Internet Portal.* Home page http://www.commoncriteriaportal.org/

[CC12] Common Criteria Sponsoring Organizations: *Common Criteria for Information Technology Security Evaluation (Version 3.1, Revision 4).* Common Criteria Recognition Arrangement (CCRA), Home page, September 2012. http://www.commoncriteriaportal.org/thecc.html

[CCDB07] Common Criteria Development Board: *Composite product evaluation for Smart Cards and similar devices, Version 1.0, Revision 1.* Common Criteria Supporting Document CCDB-2007-09-001, September 2007

[DFG+11] A. Datta, J. Franklin, D. Garg, L. Jia, and D. Kaynar: *On Adversary Models and Compositional Security.* IEEE Security & Privacy, Vol. 9, No. 3, pp. 26–32, May/June 2011

[EMILS13] *EURO-MILS Project.* Home Page. http://www.euromils.eu

[HMK12] G. Heiser, T. Murray, and G. Klein: *It's Time for Trustworthy Systems.* IEEE Security & Privacy, Vol. 10, No. 2, pp. 67–70, March/April 2012

[IAD07] Information Assurance Directorate: *U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness (Version 1.03).* June 2007 http://www.niap-ccevs.org/cc-scheme/pp/pp.cfm/id/pp_skpp_hr_v1.03/

[Kal12] J. Kallberg: *The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal.* IEEE Security & Privacy, Vol. 10, No. 4, pp. 50–53, July/August 2012.

[KKS+08] H. Kurth, G. Krummek, C. Stüble, M. Weber, M. Winandy: *HASK-PP Protection Profile for a High Assurance Security Kernel (Version 1.14).* SIRRIX AG und Bundesamt für Sicherheit in der Informationstechnik, Juni 2008

[KMP+11] P. A. Karger, S. K. McIntosh, E. R. Palmer, and D. C. Toll: *Lessons Learned Building the Caernarvon High-Assurance Operating System.* IEEE Security & Privacy, Vol. 9, No. 1, pp. 22–30, January/February 2011

[MBA12] S. J. Murdoch, M. Bond, and R. Anderson: How Certification Systems Fail: *Lessons from the Ware Report.* IEEE Security & Privacy, Vol. 10, No. 6, pp. 40–44, November/December 2012

[MPS+12] K. Müller, M. Paulitsch, R. Schwarz, S. Tverdyshev, H. Blasum: *MILS-Based Information Flow Control in the Avionic Domain: A Case Study on Compositional Architecture and Verification.* In: Proceedings 31st Digital Avionics Systems Conference (DASC), Williamsburg, VA, October 2012
(von der DASC mit "Best of Session" ausgezeichnet.)

[RG05] M. Rosenblum and T. Garfinkel: *Virtual Machine Monitors: Current Technology and Future Trends.* IEEE Computer, pp. 39–47, May 2005

[RS12] M. Rudolph, R. Schwarz: *A Critical Survey of Security Indicator Approaches.* In: Proceedings 7th International Conference on Availability, Reliability and Security (ARES2012), Prague, Czech Republic, pp. 291–300, August 2012
DOI 10.1109/ARES.2012.10

[Rus81] J. Rushby: *Design and Verification of Secure Systems.* In: Proceedings 8th ACM Symposium on Operating System Principles, Pacific Grove, California, (ACM Operating Systems Review, Vol. 15, No. 5, pp. 12–21), December 1981.

[SCRIT13] *SECCRIT Project.* Home Page. https://www.seccrit.eu/

[SeSaM11] *SeSaM Project.* Home Page. http://www.sysgo.com/company/about-sysgo/rd-projects/the-sesam-project/

[SINNO13] *SINNODIUM Project.* Home Page. http://www.software-cluster.org/de/forschung/projekte/verbundprojekte/sinnodium

[SP07] R. Schwarz, H. Peine: *Methoden, Techniken und Werkzeuge zur Entwicklung hochsicherer Software.* Report Nr. 113.07/D, Fraunhofer IESE, Kaiserslautern, Dezember 2007

[STB+12] W. Stephan, S. Tverdyshev, H. Blasum, B. Langenstein, K. Müller, A. Nonnengart, M. Paulitsch, R. Schwarz: *CC Compositional Certification for MILS Virtualization Platforms.* In: Proceedings International Common Criteria Conference (ICCC), Paris, France, September 2012

[Sysgo12] *PikeOS.* Product page, SYSGO, 2012 http://www.sysgo.com/products/pikeos-rtos-and-virtualization-concept/

[Sysgo13] S. Tverdyshev: *SeSaM: Schlussbericht des Gesamtvorhabens.* SYSGO AG, 2013

[Sysgo13b] S. Tverdyshev: *SeSaM: Erfolgskontrollbericht des Gesamtvorhabens.* SYSGO AG, 2013

[Win10] E. Winterton: *Composed TOE Lessons Learned.* Präsentation, 11th International Common Criteria Conference (ICCC), Antalya, Türkei, September 2010

Liste der Abkürzungen

ACO	Assurance Class »Composition«
AP	Arbeitspaket
BMBF	Bundesministerium für Bildung und Forschung
CAP	Component Assurance Package(s)
CC	Common Criteria for IT Security Evaluation
CCDB	Common Criteria Development Board
CCRA	Common Criteria Recognition Arrangement
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
EADS	European Aeronautic Defence and Space Company
EAL	Evaluation Assurance Level
EUROCAE	European Organization for Civil Aviation Equipment
IESE	Fraunhofer-Institut für Experimentelles Software Engineering
IMA	Integrated Modular Avionics
IT	Informationstechnologie
MILS	Multiple Independent Levels of Security
NIAP	U.S. National Information Assurance Partnership
PP	Protection Profile (Schutzprofil-Spezifikation)
RTCA	Radio Technical Commission for Aeronautics
SAR	Security Assurance Requirement (Vertrauenswürdigkeitsanforderungen)
SECCRIT	Secure Cloud Computing for Critical Infrastructure IT (EU-FP7 Projekt)
SeSaM	Secure and Safe Microkernel Made in Germany
SINNODIUM	Software-Innovationen für das digitale Unternehmen (BMBF-Projekt)
SFR	Security Functional Requirement (Funktionale Sicherheitsanforderungen)
ST	Security Target (Schutzziel-Spezifikation)
TOE	Target of Evaluation (Evaluationsgegenstand)
TSF	Target of Evaluation Security Functionality

Dokumenteninformation

Titel:	Secure and Safe Microkernel Made in Germany: Kriterien und Konzepte für eine modulare Security-Zertifizierung Safety-kritischer Virtualisierungsplattformen
Datum:	Mai 2013
Report:	026.13/D
Status:	Final
Klassifikation:	Public Unlimited