Security von sicherheitsrelevanten rechnerbasierten Systemen in Kernkraftwerken

Verfasser: Ferdinand Dafelmair / Cornelia Bühler
TÜV Industrie Service GmbH
TÜV SÜD Gruppe
München

Zusammenfassung

Der weiter fortschreitende Ausbau von informationstechnischen Systemen im Kernkraftwerk betrifft neben den verwaltungstechnischen Abläufen zunehmend auch sicherheitstechnisch bedeutende Systeme. Es werden konventionelle Leittechnikssysteme durch rechnerbasierter Pendants ersetzt, elektronische Workflow Management Systeme zur Abwicklung wichtiger administrativer Prozesse verwendet und lokale Datennetze mit externen Datennetzen gekoppelt. Dabei ist zunehmend die Frage zu stellen, wie die Rechner- und Kommunikationssysteme im Kernkraftwerk nicht nur gegen Ausfälle oder Entwicklungsfehler sondern auch gegen bewußte Manipulationen zu schützen sind. Der vorliegende Beitrag zeigt auf, in wie weit die steigende Anzahl von Angriffen auf informationstechnische Systeme und die dabei angewandten Methoden auch für die informationstechnischen Systeme in Kernkraftwerken eine Bedrohung darstellen. Darauf aufbauend werden Maßnahmen dargelegt, wie diesen Bedrohungen wirksam begegnet werden kann. Abschließend werden die neuesten Entwicklungen im Bereich der digitalen Signatur vorgestellt und aufgezeigt, wie damit auch im Zeitalter der papierlosen Vorgangsabwicklung die Urheberschaft und Integrität von wichtigen internen Dokumenten, wie z.B. Arbeitserlaubnisscheinen oder Schichtbüchern zweifelsfrei gesichert werden kann.

1. Was ist Security?

Zur näheren Bestimmung von Security ist eine Gegenüberstellung mit dem Begriff „Safety“ hilfreich, da beide Begriffe mit „Sicherheit“ ins Deutsche übersetzt werden können.

Safety betrifft hierbei die Sicherheit, daß das System die spezifizierten Funktionen korrekt ausführt, trotz Fehlern, Ausfällen oder widriger Umweltbedingungen. Die Auslegung von sicherheitsrelevanten Systemen hinsichtlich Safety wie z. B. durch Redundanz, Diversität, räumliche Trennung und Entkopplung ist in der Kerntechnik gängige Praxis.

Security ist dagegen die Sicherheit vor Manipulationen. Sie bezieht sich hierbei auf Daten und Programme, d. h. sie ist nur bei rechnerbasierten Systemen relevant. Im Gegensatz zur Safety, die unvermeidbare, unbeabsichtigte Fehler innerhalb eines Systems oder durch die Umgebung berücksichtigt, bezieht sich die Security auf vorsätzliche Schadenshandlungen von außen durch Dritte.

Das Ziel der Security ist dabei die Wahrung der folgenden Eigenschaften von Daten und Programmen eines Rechnersystems:

- **Integrität**
  Hierunter wird die Problematik der unerwünschten Änderung von Daten und Programmen verstanden.
- **Verfügbarkeit**
  Hierunter wird die Eigenschaft von Daten und Dienstleistungen verstanden, immer dann verfügbar zu sein, wenn ein autorisierter Benutzer sie bearbeiten bzw. in Anspruch nehmen will.
- **Vertraulichkeit**
  Dies beinhaltet die Forderung, daß Informationen nur den dazu autorisierten Personen zur Kenntnis gelangen dürfen.
- **Verbindlichkeit**
  Technisch werden hierunter die Authentizität von Kommunikationsinhalten sowie Fragen des Anerkennens bzw. Leugnens von Kommunikationsbeziehungen verstanden. Besondere Bedeutung hat die Verbindlichkeit für vertragliche Transaktionen, die auf elektronischem Weg zustande kommen.

Von besonderer Bedeutung sind bei den derzeit durch Rechnersysteme in Kernkraftwerken realisierten Funktionen die Verfügbarkeit von Rechnersystemen und die Integrität von Programmen und Daten sowie die Vertraulichkeit, beispielsweise von Zugangsberechtigungen wie Paßwörtern. Aspekte der Verbindlichkeit hatten für Rechnersysteme in Kernkraftwerken bis vor kurzem noch nachgeordnete Bedeutung. Im Hinblick auf die derzeit bereits laufende und zukünftig vorgesehene weitere Vernetzung von Rechnersystemen und die Einführung papierloser Arbeits- und Verwaltungsabläufe kommt jedoch auch dieser Eigenschaft eine stärkere Bedeutung zu.

2. Einsatzgebiete von Rechnersystemen in KKWs

Eine klassische Anwendung von sicherheitsrelevanten Rechnern in Kernkraftwerken stellen die Prozeßrechneranlagen zur Erfassung, Verarbeitung und Darstellung von Daten aus dem Kraftwerksprozeß dar. Neben den Prozeßrechneranlagen existieren noch weitere Systeme zur Analyse des Prozeßgeschehens und zur Archivierung der Prozeßdaten. Exemplarisch können an dieser Stelle Kernsimulatoren zur reaktorphysikalischen und thermohydraulischen Überwachung des Reaktorkerns genannt werden. Ferner werden Rechnersysteme unterschiedlicher Komplexität in zunehmendem Maß in Prüfsystemen eingesetzt. Ein weiterer Anwendungsfall für Rechnersysteme in Kernkraftwerken ist der Bereich der Anlagensicherung. Darüber hinaus finden Rechnersysteme in jüngster Zeit auch Anwendung in Sicherheitssystemen der höchsten Sicherheitskategorie wie beim Reaktorschutzsystem und bei Meßsystemen zur Erfassung der Neutronenflußdichte.

Neben den wachsenden Einsatzgebieten von Rechnersystemen in Kernkraftwerken ist auch die Struktur der Rechnsysteme im Wandel begriffen. Der allgemeinen Entwicklung in der Industrie folgend werden seit längerem auch in Kernkraftwerken in zunehmendem Maß bestehende, zentrale Rechner mit sicherheitstechnischer Bedeutung durch moderne dezentrale Rechnersysteme ersetzt. Darüber hinaus werden diesen sicherheitstechnisch relevanten Rechnersystemen entsprechend ihrer gestiegenen Leistungsfähigkeit weitere Aufgaben übertragen. Die im Kernkraftwerk vorhandenen Rechnersysteme werden miteinander verbunden, um durch gezielten Informationsaustausch zwischen den einzelnen Rechnersystemen und durch eine verbesserte, benutzerfreundlichere Mensch-Maschine-Schnittstelle Arbeitsabläufe zu rationalisieren, Daten besser auszuwerten und Synergieeffekte nutzen zu können. Durch die stark voranschreitende Vernetzung von sicherheitstechnisch relevanten Rechnersystemen sowie durch deren hohe Komplexität ergeben sich zunehmend mehr Möglichkeiten zur unbefugten Manipulation dieser Rechnersysteme, wie sie in anderen Anwendungsbereichen von Rechnersystemen zu beobachten sind.

3. Bedrohungsanalyse

Aufgabe einer **Bedrohungsanalyse** ist es, alle realen Bedrohungen zu erkennen, zu analysieren und zu dokumentieren. Hierzu ist es erforderlich, für den jeweiligen Einzelfall durch eine Analyse vor Ort durch Experten die zu unterstellenden Bedrohungen zu bestimmen. Entsprechend den Empfehlungen des BSI im IT-Grundschutzhandbuch [BSI 1] werden hierbei folgende Gruppen von Gefährdungen betrachtet:

- höhere Gewalt (Blitz, Feuer, Wasser, Kabelbrand etc.)
- organisatorische Mängel (z.B. fehlende oder unzureichende Regelungen)
- menschliche Fehlhandlungen (z. B. Nichtbeachtung von IT-Sicherheitsmaßnahmen)
- technisches Versagen (z. B. Fehler in Betriebssystemen)

- vorsätzliche Handlungen (Manipulationen)

Die eigentliche Bedrohung der Rechnersysteme in Sinne der Security besteht in den vorsätzlichen Handlungen, die durch die anderen genannten Bedrohungen gegebenenfalls begünstigt werden. Die vorsätzlichen Handlungen können aktive oder passive Angriffe darstellen. Passive Angriffe sind z. B.

- Abhören der Kommunikation im Netzwerk oder
- Verkehrsflußanalyse mit Netzanalyse-Tools.

Aktive Angriffe erfordern fast immer vorangehende passive Angriffe, um sich Informationen bezüglich des anzugreifenden Systems oder Netzwerkes zu beschaffen. Beispiele für aktive Angriffe sind:

- Zugangsmöglichkeiten durch Ausnutzung von Netzwerkdiensten
- systematisches Ausprobieren von Paßwörtern
- Maskerade
- Computer-Viren
- Würmer und trojanische Pferde
- IP-Spoofing
- Denial of Service Angriff
- Angriff auf Netzwerkfunktionen (Router, Gateway, etc.)
- Mißbrauch von Fernwartungszugängen

Für die beispielhaft aufgelisteten Bedrohungen von Rechnersystemen lassen sich folgende allgemeine Bedrohungscharakteristika identifizieren:

- Ausweitung der Zugriffsmöglichkeit

Sind Rechnersysteme über ein Kommunikationsnetzwerk vernetzt, kann prinzipiell von jedem Rechner im Netzwerk auf andere Rechner im Netzwerk zugegriffen werden. Dieser Zugriff ist auch dann möglich, wenn der Angreifer lediglich physischen Zugang zur Verkabelung des Netzwerkes besitzt, da er in diesem Fall mitgebrachte portable Rechnersysteme unerlaubt in das Netzwerk einbinden kann. Passworte schützen nicht vor derartigen Bedrohungen. Damit kann der physische Zugriffsschutz umgangen werden und es können auch Personen auf zu schützende Systeme zugreifen, denen kein physisches Zugriffsrecht eingeräumt wurde.

- Anonymität des Zugriffs und Senkung des Aufdeckungsrisikos

Da der Zugriff von beliebiger Stelle im Netzwerk, ggf. sogar von außerhalb der Anlage aus erfolgen kann, und im Unterschied zu klassischen Systemen kein physischer Zutritt zu physisch gesicherten Bereichen erforderlich ist, kann eine Manipulation anonym erfolgen. Da bei dieser anonymen Vorgehensweise ein weitaus geringeres Aufdeckungsrisiko als bei Manipulation von Systemen vor Ort zu befürchten ist, ist die Hemmschwelle für derartige Tätigkeiten ebenfalls niedriger anzusetzen.

- Schwierige Detektierbarkeit von Manipulationen

Heutige Rechnersysteme mit marktüblichen Betriebssystemen verfügen über eine hohe Komplexität und vielfältige Möglichkeiten zur Beeinflussung. Manipulationen und Eindringversuche hinterlassen zwar ebenso wie mechanische Eindringversuche an abgeschlossenen Einheiten Spuren, nur sind diese im allgemeinen entweder schwer zu erkennen oder sie können von den Angreifern selbst nahezu vollständig beseitigt werden. Da viele Funktionen eines Systems nicht stets im Eingriff sind, können durch Manipulationen hervorgerufene Fehlfunktionen mit funktionshemmender Charakteristik erst im Anforderungsfall detektiert werden.

- Erweiterung der Zeitdauer für Manipulationen

Im Gegensatz zu Manipulationen vor Ort besteht bei Manipulationen über Kommunikationsnetzwerke oder im Rahmen des Erstellungsprozesses von Software nahezu keine Einschränkung hinsichtlich der Zeitdauer für Manipulationen. Durch gezielte Systembeobachtung und Versuche hat der Angreifer zusätzlich die Chance, die Systemfunktionen genau zu studieren, seine Manipulation über lange Zeit hinweg genau zu planen und ggf. sogar die beabsichtigte Wirkung am System selbst zu testen, ohne daß dies auffallen würde, da er die Spuren seines Tuns u.U. verwischen kann.

- Zeit- oder ereignisgesteuerte Triggerung von Störfunktionen

Im Vergleich zu klassischer, nicht programmierbarer Leittechnik weisen Rechnersysteme einen hohen Funktionalitäts- und Performance-Overhead auf. Diesen kann der Angreifer dazu nutzen, gezieltes, von ihm gewünschtes Funktionsverhalten zusätzlich zu den spezifizierten Funktionen zu implementieren und dadurch zeit- oder ereignisgetriggert seine Störfunktionen dann aktiv werden zu lassen, wenn die von ihm beabsichtigte Wirkung (z.B. Schadenswirkung) maximal ist.

4. Security-Planung

4.1 Security-Grundsätze

Um neue Rechner- und Kommunikationstechnik in Kernkraftwerke einbringen zu können und die damit verbundenen Synergieeffekte nutzen zu können, muß den bei diesen Systemen neu zu betrachtenden Bedrohungen in Bezug auf vorsätzliche Manipulationen wirksam begegnet werden. Wie diese Aufgabe im konkreten Einzelfall gelöst wird, kann nach dem Stand der Technik nur anlagenspezifisch in einem Security-Konzept dargestellt werden, welches die speziellen Gegebenheiten der Anlage berücksichtigt. Im Sinne eines generischen Security-Konzeptes werden die nachfolgend genannten Auslegungsgrundsätze zur Security definiert, die für alle sicherheitsrelevanten rechnerbasierten Systeme relevant sind.

- Security-relevante Rechnersysteme (SRS) sollen so ausgelegt sein, daß sie zumindest einen Aufdeckungsgrad für Manipulationen besitzen, der in Bezug auf das spezifizierte Funktionsverhalten mindestens dem der bisherigen Technologie bzw. Verfahren entspricht. Dabei kann von Sicherungsfunktionen zur Manipulationsvermeidung Kredit genommen werden.

- Technische Maßnahmen zur Zugriffskontrolle für SRS sind so zu gestalten, daß sie den Zugriff auf SRS nachweislich auf die dazu speziell autorisierten Personen beschränken, wobei jeder Person nur die ihr zugebilligten Rechte zur Ausführung bestimmter Funktionen eingeräumt werden dürfen.

- Die SRS sind derartig zu konzipieren, daß Verantwortungsbereiche für die Integrität von SRS eindeutig und rechtlich abgesichert bestimmten Personen in einer der bisherigen Vorgehensweise entsprechenden Art und Weise zugewiesen werden können.

Für Rechnersysteme im Bereich der Sicherheitsleittechnik, die zur sicheren Beherrschung des kerntechnischen Prozesses dienen, ist darüber hinaus folgender Grundsatz zu berücksichtigen:

- Rechnersysteme im Bereich der Sicherheitsleittechnik sind derart auszulegen, daß keine Manipulationen durchführbar sind, die ein Versagen des Gesamtsystems zur Folge haben. Dabei sind Security-Schutzfunktionen deterministisch in Bezug auf zu unterstellende Schadenspotentiale im Falle ihres Versagens auszulegen.

4.2 Security-Zonen

Bei der Security-Planung ist es zweckmäßig, Security-Zonen zu definieren, wobei Systeme mit vergleichbarem Schutzbedarf in gemeinsamen Zonen zusammengefaßt werden. Unter vergleichbarem Schutzbedarf ist hierbei zu verstehen, daß vergleichbare Anforderungen an technische und administrative Schutzmaßnahmen zu stellen sind und die Systeme in einer Zone auch hinsichtlich der Benutzergruppen und der Anforderungen an deren Vertrauenswürdigkeit kompatibel sind. Durch die Zonenbildung kann erreicht werden, daß die Zugriffsschutzmaßnahmen innerhalb der Zonen vereinheitlicht werden können und damit die Zone als Ganzes mit Schutzmaßnahmen ausgestattet werden kann anstatt einzelne Systeme innerhalb der Zone für sich zu schützen. Dadurch verringert sich die Anzahl der Schnittstellen zwischen Bereichen unterschiedlicher Sicherheitsanforderungen, wodurch Ressourcen eingespart werden können und ein gestaffelter Schutz in Form von mehreren, ineinander geschachtelten Zonen möglich ist. Bei der Zonenbildung ist zu unterscheiden zwischen **konkreten** und **abstrakten** Security-Zonen.

Konkrete Security-Zonen sind Security-Zonen, die über ihre örtliche Lage, Ausdehnung und Barrieren an der Zonengrenze definiert sind, wobei die Barrieren sowohl physischer als auch datentechnischer Natur sind. Sie beruhen auf dem Paradigma der Abgrenzung von Systemen mit schützenswertem „Inhalt“ inklusive ihrer Kommunikationskanäle untereinander gegenüber Bedrohungen von außerhalb der Security-Zone. Physische Barrieren (z.B. alle baulichen Maßnahmen) dienen dazu, physischen Zugriff auf die Zone und ihre zu schützenden Systeme, d.h. Zutritt von unbefugten Personen, zu verhindern. Datentechnische Barrieren, z.B. Firewalls Systeme, verhindern unbefugten datentechnischen Zugang über Kommunikationswege (Netzwerke, Datenträgeraustausch etc.).

Im Gegensatz zu konkreten Security-Zonen werden abstrakte Security-Zonen nur über die Ressourcen definiert, über die Anwender eines Systems verfügen müssen, um auf die Systeme einer abstrakten Zone bzw. genauer deren Daten und Funktionen zugreifen zu können. Ressourcen sind hierbei Wissen, Besitz oder unveränderbare persönliche Merkmale bzw. eine Kombination davon. Ein weiteres Merkmal abstrakter Security-Zonen ist, daß nicht Systeme, sondern deren „Inhalt“, d.h. die Programme und Daten selbst geschützt werden. Dies geschieht durch Verwendung kryptografischer Algorithmen, die mit Hilfe von Schlüsseln eine Chiffrierung von Daten vornehmen. Nur wer über die Schlüssel, d.h. einen Code aus Bitfolgen, verfügt, erhält Zugriff auf die Daten und damit Zugang zu der entsprechenden abstrakten Zone.

Die nachfolgende Darstellung einer abstrakten Zonenbildung (Abb. 1) ist generisch und versucht möglichst allgemeingültig den heutigen Stand der Realisierung und Planung in Kernkraftwerken abzubilden.

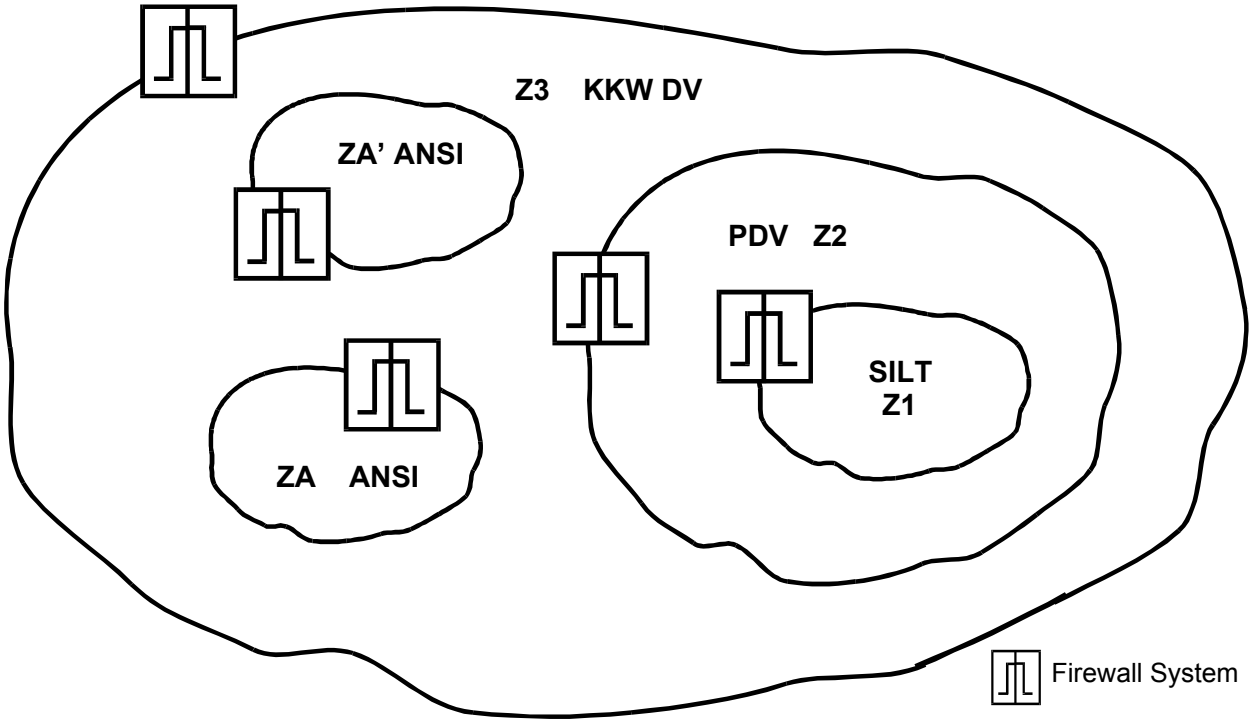

Abb. 1: Generische Darstellung der Zonenbildung in Kernkraftwerken

Zone Z1
Innerste Security-Zone für die Sicherheitsleittechnik (SILT), der typischerweise die folgenden Systeme zugeordnet sind:
- Reaktorschutzsystem
- Systeme für sicherheitstechisch wichtige Begrenzungsfunktionen
- Prüf- und Diagnosesysteme für Sicherheitsleittechnik

Zone Z2
Security-Zone für die Rechnersysteme der Prozeßdatenverarbeitung (PDV). Ihr sind zugeordnet:
- Systeme zur Regelung und Begrenzung
- Systeme der Online-Verfolgung des Kernzustandes
- Prozeßinformationssysteme
- Datenaufzeichnungssysteme
- Systeme zur Führung des Schichtbuches
- Systeme zur Vorhaltung und Abfrage des elektronischen Betriebshandbuches

Zone Z3
In dieser Security-Zone finden sich alle nichttechnischen und betrieblichen Systeme zur Datenverarbeitung (DV) eines Kernkraftwerkes inkl. der Systeme zur Durchführung wichtiger Offline-Berechnungen sowie die nicht der Zone Z2 zugeordneten Systeme zur Abwicklung adminstrativer Prozesse.

Zonen ZA und ZA'
In diesen Zonen befinden sich die zentralen Systeme der Anlagensicherung (ANSI). Dabei ist zu berücksichtigen, daß die Systeme der Anlagensicherung hinsichtlich der Mensch-Maschine-Schnittstelle zur Dateneingabe und Überwachung auf Pfortenbereiche und Sicherheitszentrale aufgeteilt sind und die zentralen Server der Systeme in mehreren separaten Zonen (ZA, ZA') untergebracht sind.

4.3 Schutzphilosophie

Um wirkungsvoll vorsätzlichen Manipulationen an SRS begegnen zu können, sind zwei Aspekte zu berücksichtigen. Zum einen müssen Manipulationen so früh wie möglich erkannt werden, um auf sie reagieren und ihre Auswirkungen begrenzen zu können. Hierzu sind entsprechende Maßnahmen zur Erkennung von Angriffen, z.B. Selbstüberwachungsmechanismen, zu realisieren. Zum anderen müssen für einen Teil der Rechnersysteme zur Einhaltung der definierten Security-Schutzziele über die Maßnahmen zur Erkennung von Angriffen hinaus Maßnahmen zur Vermeidung von Manipulationen getroffen werden.

Eine absolute Vermeidung von Manipulationen an DV-Systemen ist nach heutigen Erkenntnissen nicht möglich, da mit genügend Ressourcen (Rechnerleistung, Zeit, Geld und Know-How, etc.) jede Schutzmaßnahme überwunden werden kann. Für die Bewertung der Wirksamkeit einer Schutzmaßnahme gegen Manipulation ist daher stets zu berücksichtigen, welche Ressourcen einem Angreifer zur Verfügung stehen.

Die Wirksamkeit von Schutzmaßnahmen zur Vermeidung von Manipulationen sollte so gewählt werden, daß die für einen erfolgreichen Angriff auf ein SRS erforderlichen Ressourcen dem Schutzbedarf der SRS angepaßt sind. Der Schutzbedarf wird durch deterministische Ermittlung des Schadens bestimmt, der entsteht, wenn ein Angriff erfolgreich durchgeführt werden kann. So ist z.B. die Wirksamkeit von Schutzmaßnahmen in der Security-Zone Z1 so zu gestalten, daß nur noch wenige Spezialisten mit einem großen Aufwand an Ressourcen in der Lage sind, die aufgebauten technischen Barrieren zum Schutz von SRS gegen Manipulationen zu überwinden.

Für Systeme mit geringerem Schutzbedarf ist beispielsweise sicherzustellen, daß die Schutzmaßnahmen wirksam sind gegenüber Angriffen, die mit allgemein zugänglichen Hilfsmitteln und mit z.B. frei aus dem Internet zugänglicher Software und Know-How-Unterstützung von einem großen Kreis an potentiellen Angreifern ausgeführt werden können.

4.4 Abgestufte Schutzmaßnahmen

Ausgehend von den Security-Grundsätzen können nunmehr konkrete Schutzmaßnahmen gegen Manipulationen an SRS definiert werden, die in ihrer Wirksamkeit den Anforderungen an bereits im technischen Regelwerk definierte und in den Anlagen umgesetzte Schutzmaßnahmen gegen technisches Versagen entsprechen.

Zur Abstufung der Schutzmaßnahmen empfiehlt sich eine Gliederung nach folgendem Schema:

- Grundlegende Schutzmaßnahmen
- Erweiterte Schutzmaßnahmen
- Restriktive Schutzmaßnahmen

Die grundlegenden Schutzmaßnahmen finden auf alle sicherheitsrelevanten rechnerbasierten Systeme in einem Kernkraftwerk Anwendung. Die erweiterten Schutzmaßnahmen sind nur für die Rechnersysteme der Zonen Z1 und Z2 von Bedeutung. Die restriktiven Schutzmaßnahmen werden nur auf Rechnersysteme der Zone Z1 angewendet.

Die konkreten Schutzmaßnahmen leiten sich ab aus dem Stand der Technik für industrielle und kommerzielle Anwendungen von Rechnersystemen und Kommunikationsnetzen, wie er sowohl in Empfehlungen staatlicher Behörden (vgl. [BSI 1]), in nationalen und internationalen Kriterienwerken (vgl. [ITSEC 1], [TCSEC 1], [NATO 1], [Fed Cr 1], [CTCPEC 1]) als auch in den einschlägigen Sicherheitsempfehlungen von Systemherstellern dokumentiert ist und wie er aus Referenzinstallationen abgeleitet werden kann. Ferner fließen hierin die Erkenntnisse aus der systematischen Auswertung bekannter erfolgreicher Manipulationsszenarien mit ein.

Aufgrund der schnell voranschreitenden Entwicklung der Informationstechnik ergeben sich ständig neue Manipulationsmöglichkeiten, und die technischen Ressourcen der Angreifer wachsen kontinuierlich an. Als Folge dieser Tatsache müssen auch die Schutzmaßnahmen regelmäßig bezüglich ihrer Wirksamkeit überprüft und gegebenenfalls erweitert werden.

Security von sicherheitsrelevanten rechnerbasierten Systemen in Kernkraftwerken

Verfasser: Ferdinand Dafelmair / Cornelia Bühler
TÜV Industrie Service GmbH
TÜV SÜD Gruppe
München

Zusammenfassung

Der weiter fortschreitende Ausbau von informationstechnischen Systemen im Kernkraftwerk betrifft neben den verwaltungstechnischen Abläufen zunehmend auch sicherheitstechnisch bedeutende Systeme. Es werden konventionelle Leittechnikssysteme durch rechnerbasierter Pendants ersetzt, elektronische Workflow Management Systeme zur Abwicklung wichtiger administrativer Prozesse verwendet und lokale Datennetze mit externen Datennetzen gekoppelt. Dabei ist zunehmend die Frage zu stellen, wie die Rechner- und Kommunikationssysteme im Kernkraftwerk nicht nur gegen Ausfälle oder Entwicklungsfehler sondern auch gegen bewußte Manipulationen zu schützen sind. Der vorliegende Beitrag zeigt auf, in wie weit die steigende Anzahl von Angriffen auf informationstechnische Systeme und die dabei angewandten Methoden auch für die informationstechnischen Systeme in Kernkraftwerken eine Bedrohung darstellen. Darauf aufbauend werden Maßnahmen dargelegt, wie diesen Bedrohungen wirksam begegnet werden kann. Abschließend werden die neuesten Entwicklungen im Bereich der digitalen Signatur vorgestellt und aufgezeigt, wie damit auch im Zeitalter der papierlosen Vorgangsabwicklung die Urheberschaft und Integrität von wichtigen internen Dokumenten, wie z.B. Arbeitserlaubnisscheinen oder Schichtbüchern zweifelsfrei gesichert werden kann.

öffentlichen Schlüssel erhält der Empfänger über das Signierschlüssel-Zertifikat, das z. B. dem Dokument angehängt sein kann. Durch einen Vergleich des Hash Values des bei dem Empfänger angekommenen Dokuments mit dem verschlüsselt übertragenen, entschlüsselten Hash Value kann die Integrität des Dokuments geprüft werden. Ebenso wird damit auch die Urheberschaft nachgewiesen, da nur ein mit dem geheimen Schlüssel des Absenders verschlüsselter Wert mit dessen öffentlichen Schlüssel wieder korrekt entschlüsselt werden kann. Zur Überprüfung der Zuordnung des Absenders zu dem öffendlichen Schlüssel kann der Empfänger die Richtigkeit und Gültigkeit des Zertifikates beim Trust Center verifizieren.

Aus den vorangehenden Ausführungen kann gefolgert werden, daß im Kernkraftwerk die Sicherstellung der Qualitätsmerkmale Integrität und Verbindlichkeit bei administrativen Prozessen nach Ablösung der Papierdokumente durch Dokumente in elektronischer Form nicht mehr automatisch gegeben ist, sondern durch technische Mittel erreicht werden muß. Damit bekommen diese betrieblichen administrativen Prozesse, wie die rechnerbasierten sicherheitsrelevanten Funktionen des Kernkraftwerkes, eine Relevanz hinsichtlich Security. Zur Sicherstellung der Verbindlichkeit der elektronisch geleisteteten Unterschriften ist es daher notwendig auch die Rechnersysteme, die die Abwicklung dieser administrativen Prozesse realisieren, einer Bewertung der Security zu unterziehen.

6. Resümee

Durch die Zunahme der Komplexität und die Erweiterung der Funktionalität der eingesetzten Rechnersysteme, die ihrerseits untereinander über leistungsfähige, standortübergreifende Kommunikationssysteme vernetzt sind und vielfach auch eine Anbindung an externe Datennetze besitzen, sind neue rechnerspezifische Versagensmechanismen (Bedrohungen)zu betrachten. Diese Bedrohungen ergeben sich sowohl aufgrund technischer Defekte, die ihre Ursache in physikalischen Effekten oder von Menschen verursachten Fehlhandlungen haben können, als auch aufgrund von vorsätzlichen Manipulationen, die bei der bisherigen Technik noch keine besondere Rolle gespielt haben.

Aufgrund der überaus schnellen Weiterentwicklung der Rechnertechnik und deren zunehmender Komplexität treten ständig neue Manipulationsmöglichkeiten auf. Außerdem wachsen die technischen Ressourcen der Angreifer kontinuierlich an, wobei diese Ressourcen aufgrund des rapiden Preisverfalls in der Informationstechnik einer immer größeren Zahl von potentiellen Angreifern zur Verfügung stehen. Es kommt damit zu einem ständigen Wettrüsten zwischen den Security-Spezialisten, die mit Schutzmaßnahmen Angriffe auf ihre Rechnersysteme unmöglich machen bzw. diese zumindest erkennen möchten, und den Angreifern, die mit immer ausgefeilteren Angriffstechniken aus den unterschiedlichsten Gründen zum Ziel haben, diese Rechnersysteme zu manipulieren. Um im Wettrüsten mit den Angreifern die Rechnersysteme und Kommunikationsnetze wirksam vor Manipulationen schützen zu können, müssen sowohl die eingesetzten Ressourcen als auch das Know How zu diesen Spezialthemen stets auf dem aktuellen Stand gehalten werden.

In zunehmendem Maße werden Rechnersysteme in Kernkraftwerken auch zur Abwicklung wichtiger administrativer Prozesse wie Freischaltwesen, Arbeitserlaubnisscheinwesen etc. eingesetzt, wobei insbesondere auch Unterschriften, die bisher auf dem Papier geleistet wurden, zukünftig elektronisch gegeben werden. Werden derartige Systeme nicht sehr sorgfältig geplant, implementiert und stets auf dem aktuellen Stand der Technik gehalten, können Fälschungen dieser Unterschriften bzw. der unterschriebenen Dokumente mehr oder weniger leicht vorgenommen werden. Damit wird es zunehmend schwieriger, die Verantwortung für Entscheidungen oder Handlungen einzelnen Personen im Betriebsablauf eines Kraftwerkes eindeutig zuzuweisen.

7. Literatur

[BSI 1] Bundesamt für Sicherheit in der Informationstechnik
IT-Grundschutzhandbuch
Maßnahmenempfehlungen für den mittleren Schutzbedarf
Stand: 1995, Bundesanzeiger Verlag

[Kers 1] Heinrich Kersten
Sicherheit in der Informationstechnik
Einführung in Probleme, Konzepte und Lösungen
2. Auflage 1995, Oldenbourg Verlag

[Pohl 1] Norbert Pohlmann
Firewalls-Systeme
Sicherheit für Internet und Intranet
1. Auflage, 1997, International Thomson Publishing Company

[Cam 1] Debra Cameron
Security Issues for the Internet and the World Wide Web
1st edition, 1996, Computer Technology Research Corp.

[Stal 1] William Stallings
Sicherheit im Datennetz
1995, Prentice Hall Verlag

[ITSEC 1] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)
Vorläufige Form der harmonisierten Kriterien
Version 1.2, Juni 1991, Bundesanzeiger Verlag

[Fed Cr 1] Federal Criteria for Information Technology Security
NIST/NSA, Stand: 1992

[NATO 1] NATO Trusted Computer System Evaluation Criteria
NATO, AC/25-D/1027, Stand: 1987

[TCSEC 1] Trusted Computer System Evaluation Criteria,
US Department of Defense, DOD 5200.28-STD, Stand: 1985

[CTCPEC 1] The Canadian Trusted Computer Product Evaluation Criteria,
Version 3.0e
Canadian Systems Security Centre - Communications Security Establishment, Government of Canada, 1992

[IEC 61226] DIN IEC 61226
Sicherheitsleittechnik - Kategorisierung
Fassung 07/97

[CT 8 98] Richard Sietmann
Augen auf, Finger gezeigt !
Erkennungssysteme auf biometrischer Basis werden praxisreif
c´t 1998, Heft 8, S. 100ff

[CERT94-08] CERT Advisories
CA-94.08 vom 14.04.1994

SigGes Informations- und Kommunikationsdienste-Gesetz (IuKDG) §3: Signaturgesetz

[DAF 1] Ferdinand J. Dafelmair
Implementation of a Security Policy in Distributed Safety Related I&C Systems - A Case Study
Safecomp 96 Proceedings, Springer London, 1996

[DAF 2] Ferdinand J. Dafelmair
Model and Implementation of a Secure SW-Development Process for Mission Critical Software
wird erscheinen in der Reihe „Lecture Notes in Computer Science“ bei Springer Heidelberg, 1998 als Beitrag zur Safecomp 98

Für weitere Informationen:

TÜV Industrie Service GmbH
TÜV SÜD Gruppe
Cornelia Bühler
Westendstraße 199
D-80686 München
Deutschland

Telefon. +49 89 5791/2315
Fax: +49 89 5791 2902
e-Mail: Cornelia.Buehler@tuev-sued.de