BAM
Bundesanstalt für Materialforschung und -prüfung

Sicherheit in Technik und Chemie

KAS

25.09.2019

LEITSÄTZE DER KOMMISSION FÜR ANLAGENSICHERHEIT (KAS) ZUM SCHUTZ VOR CYBERPHYSISCHEN ANGRIFFEN

Prof. Dr. Thomas Schendler

Stellv. Vorsitzender der KAS

5. LfULG-Kolloquium „Anlagensicherheit/Störfallvorsorge
Dresden, 25.09.2019

Kommission für Anlagensicherheit (KAS)
www.kas-bmu.de

Publikationen Gremien Intern Veranstaltungen Links Geschäftsstelle Newsletter KAS

Startseite

KAS / Startseite

Aktuell

TRAS 120

Sicherheitstechnische Anforderungen an Biogasanlagen

Weiterlesen ...

Ergänzung zum KAS-18

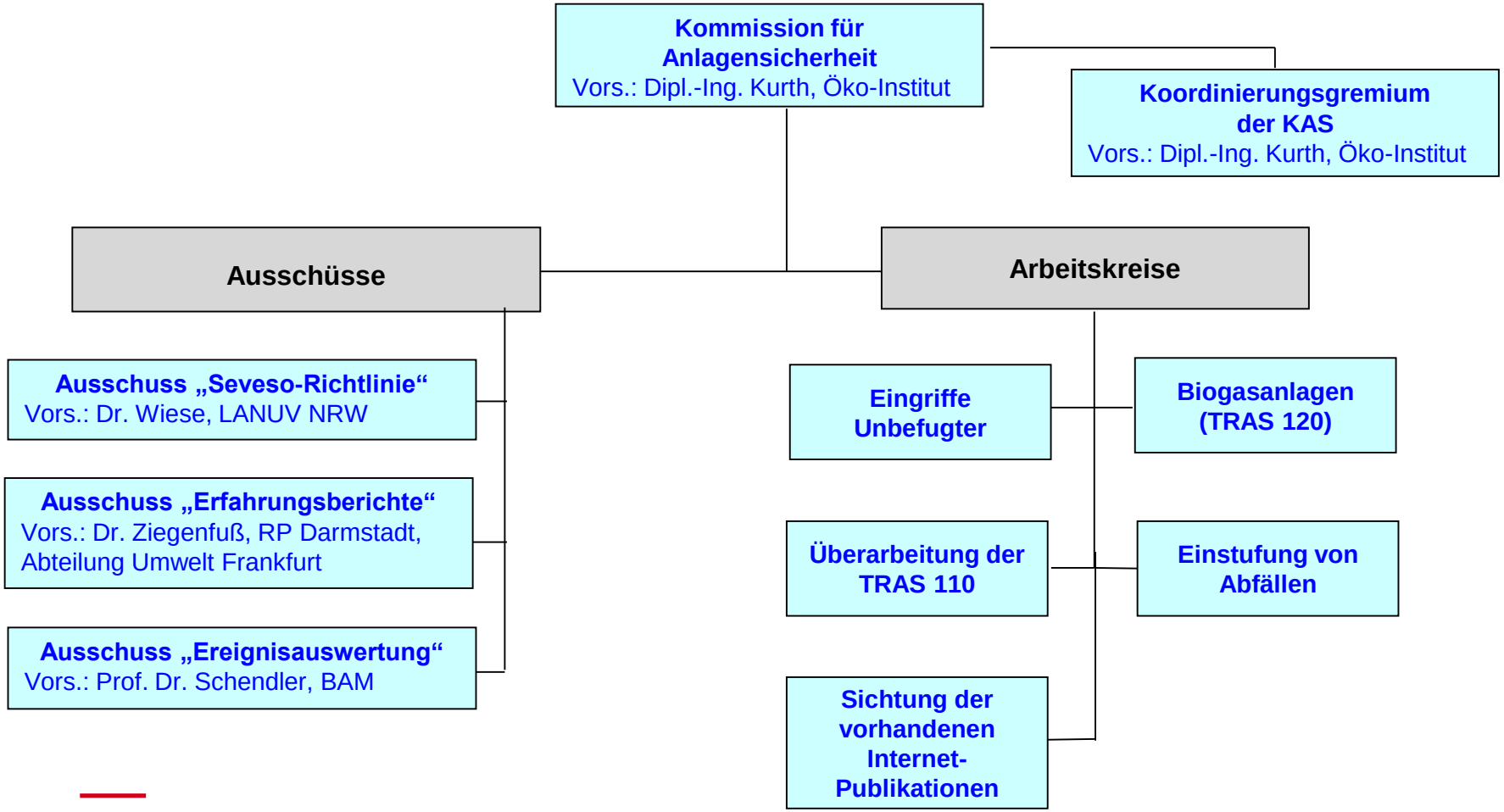
Empfehlung der KAS zu angemessenen Sicherheitsabständen bei explosiven Stoffen

Weiterlesen ...

Kommission für Anlagensicherheit (KAS)

beim Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit

Aktuelles Organigramm der KAS für die Berufungsperiode 2017-2020



KAS-Arbeitsprogramm 2017-2020

https://www.kas-bmu.de/files/Aktuelles%20Arbeitsprogramm/KAS_AP5BP.pdf

- Fertigstellung einer Technischen Regel Anlagensicherheit 120 „Sicherheitstechnische Anforderungen an Biogasanlagen".
- Überprüfung und Aktualisierung der Technischen Regel Anlagensicherheit 110 „Sicherheitstechnische Anforderungen an Ammoniak-Kälteanlagen".
- Gemeinsame Überprüfung und Aktualisierung der Technischen Regeln Anlagensicherheit 310 „Vorkehrende Maßnahmen wegen der Gefahrenquellen Niederschläge und Hochwasser" und 320 „Vorkehrende Maßnahmen wegen der Gefahrenquellen Wind sowie Schnee- und Eislasten".
- **Neufassung des Leitfadens SFK-GS-38 „Maßnahmen gegen Eingriffe Unbefugter".**

Maßnahmen gegen Eingriffe Unbefugter

Sonder-Kolloquium der KAS im Rahmen ihrer Sitzung am 21./22 Juni 2016

Thema: Cyberattacken auf Industrieanlagen

- Cyber-Security in der Industrie (BSI)
- IT-Sicherheitsanforderungen bei Industrie 4.0/Digitalisierung (Industrie)
- Drohnen-Information, Nutzen und Gefahren (Behörde)

→ Einrichtung eines Arbeitskreises der KAS zur weiteren Bearbeitung der Themen

- Cyberattacken auf Industrieanlagen
- Drohnenangriffe auf Industrieanlagen

Maßnahmen gegen Eingriffe Unbefugter

Ergebnisse des Arbeitskreises:

- Merkblatt KAS-44
  Leitsätze der Kommission für Anlagensicherheit
  zum Schutz vor cyberphysischen Angriffen

- Merkblatt KAS-45
  Hinweise der Kommission für Anlagensicherheit
  zu Drohnenangriffen auf Betriebsbereiche nach StörfallV

(von der KAS verabschiedet und veröffentlicht im Nov. 2017
https://www.kas-bmu.de/kas-merkblaetter.html)

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen

- IT-Security ist Führungsaufgabe
- Sensibilisierung und Unterweisung
- Asset Register und Netzwerkarchitektur
- IT-Security bei der Errichtung von Anlagen
- Risikomanagement beim Betrieb von Anlagen
- Erkennung von IT-Securityvorfällen
- Maßnahmen nach IT-Securityvorfällen

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen

Leitsatz 1: IT-Security ist Führungsaufgabe

- Die Leitung der Organisation ist für die IT-Security in der Organisation verantwortlich.
- Die Leitung der Organisation erstellt eine IT-Security-Richtlinie für die Organisation.
- Die IT-Security-Richtlinie ist regelmäßig an veränderte interne und externe Rahmenbedingungen anzupassen.
- In der IT-Security-Richtlinie legt die Leitung die IT-Security-Ziele der Organisation in Abhängigkeit von der Strategie der Organisation und von relevanten gesetzlichen Anforderungen fest.
- Zur Erreichung der IT-Security-Ziele schafft die Leitung geeignete Organisationsstrukturen und Prozesse.

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen

Leitsatz 2: Sensibilisierung und Unterweisung

- Die Leitung kommuniziert die IT-Security-Richtlinie an alle Mitarbeiter und alle Dritte, welche die IT-Security der Organisation unmittelbar beeinflussen können.
- Die Leitung führt geeignete Maßnahmen zur zielgruppenspezifischen Sensibilisierung der Mitarbeiter und Dritter bezüglich der Risiken, die sich aus Cyberangriffen auf Betriebsbereiche und deren Auswirkungen auf die funktionale Sicherheit auf die Organisation ergeben können, durch.
- Zur Etablierung der betrieblichen Security-Kultur werden alle Mitarbeiter und Dritte regelmäßig in den Maßnahmen zur Erreichung der Sicherheitsziele geschult und unterwiesen.
- Dritte können im Rahmen der üblichen Sicherheitseinweisung unterrichtet werden.
- Die Effektivität der Maßnahmen wird regelmäßig überprüft.

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen

Leitsatz 3: Asset Register und Netzwerkarchitektur

Nach § 3 Absatz 2 Nr. 3 der StörfallV hat der Betreiber bei der Festlegung von Vorkehrungen zur Verhinderung von Störfällen Eingriffe Unbefugter zu berücksichtigen. Relevant im Sinne der IT-Security sind solche Teile und Komponenten von Anlagen (Assets), deren Manipulation durch einen Cyberkriminellen eine mittelbare oder unmittelbare Auswirkung auf die funktionale Sicherheit der Anlage hat. Assets können sein:

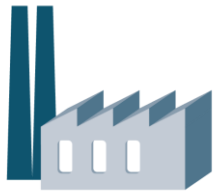
- sicherheitsrelevante Anlagenteile, Komponenten, Bauteile;
- sicherheitsrelevante Software;
- alle Netzwerk-Ein- und Ausgangspunkte zu anderen Netzwerken;
- alle IT-Systeme außerhalb des Produktionsbereiches, von denen eine Kommunikationsbeziehung in den Produktionsbereich aufgebaut werden kann;
- alle den Betriebsbereich betreffende sicherheitsrelevante Dokumentation

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen

… Leitsatz 3: Asset Register und Netzwerkarchitektur

- Zur Erfassung aller Assets ist es zweckmäßig ein Asset Register anzulegen. Für jedes Asset ist ein Verantwortlicher und der Schutzbedarf des Assets für den Betriebsprozess festzulegen.
- Zur Darstellung der Kommunikationsbeziehungen zwischen den Assets ist ein Netzwerk-Architekturbild anzufertigen. Sämtliche Übertragungsprotokolle sind bei der Darstellung der Kommunikationsbeziehungen zu berücksichtigen.
- Das Asset Register und das Netzwerkarchitekturbild sind bei Änderungen im Betriebsbereich, insbesondere bei strukturellen Änderungen, umgehend zu aktualisieren.

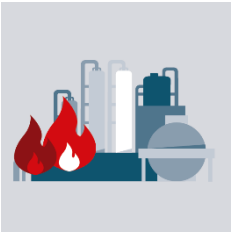
Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen



Leitsatz 4: IT-Security bei der Errichtung von Anlagen

- IT-Security ist integraler Bestandteil aller Errichtungsphasen von Anlagen und ihre Integration in den Betriebsbereich bis zur Inbetriebnahme durch den Betreiber. Sie ist integraler Bestandteil der Systemfunktionen eines Betriebsbereiches.
- Anforderungen an die IT-Security werden in der Konzeptphase vom Betreiber in Abhängigkeit von der IT-Security-Richtlinie der Organisation formuliert und in den folgenden Phasen vom Systemintegrator detailliert und umgesetzt.
- Die Erfüllung der Anforderungen an die IT-Security wird zum Ende jeder Errichtungsphase vom Systemintegrator in Zusammenarbeit mit dem Betreiber verifiziert und validiert. Vor der Inbetriebnahme erfolgt die abschließende IT-Securityabnahme durch den Betreiber.

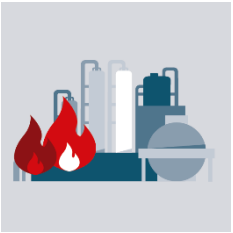
Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen



Leitsatz 5: Risikomanagement beim Betrieb von Anlagen

- Zur dauerhaften Gewährleistung der IT-Security ist ein Risikomanagement (angelehnt z. B. an ISO 27005) aufzubauen.
- Kern des Risikomanagements ist die Risikobeurteilung bestehend aus Risikoidentifizierung, Risikoanalyse und Risikobewertung.
- Grundlage für die Risikoidentifizierung sind, auf der Basis des Asset-Registers, die aktuell vorhandenen Gefährdungen für den Betriebsbereich.
- Mit der Risikobeurteilung wird die Effektivität der vorhandenen Schutzmaßnahmen in Bezug auf die aktuellen Risiken bewertet. Sofern die vorhandenen Schutzmaßnahmen die aktuellen Risiken nicht effektiv mindern sind geeignete Maßnahmen zur effektiven Minderung zu implementieren.

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen



… Leitsatz 5: Risikomanagement beim Betrieb von Anlagen

- Die Risikobeurteilung muss regelmäßig wiederholt werden, da ständig neue Schwachstellen bei vorhandenen Assets entdeckt und neue Angriffswege erfunden werden. Sollten neue, höchst kritische Schwachstellen bekannt werden, für die bereits neue Angriffswege bekannt gemacht wurden, so ist die Risikobeurteilung für die betroffenen Assets umgehend zu wiederholen.

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen

Leitsatz 6: Erkennung von IT-Securityvorfällen

- Nach § 3 Absatz 1 der StörfallV haben Betreiber erforderliche technische und organisatorische Schutzvorkehrungen zu treffen um Störfälle zu verhindern. Die rechtzeitige Detektion von IT-Securityvorfällen ist Grundvoraussetzung für die Einleitung von wirksamen Gegenmaßnahmen.
- Darüber hinaus kann die Analyse von IT-Securityvorfällen dazu dienen, geeignete Maßnahmen zur zukünftigen Vermeidung derartiger Vorfälle treffen zu können. Die Erkenntnisse fließen in das Risikomanagement ein.
- Im Sicherheitsmanagementsystem sind daher geeignete Maßnahmen zur effizienten Erkennung und Meldung von IT-Securityvorfällen zu ergreifen.

Leitsätze der KAS zum Schutz vor cyberphysischen Angriffen

Leitsatz 7: Maßnahmen nach IT-Securityvorfällen

- Im Sicherheitsmanagementsystem sind geeignete Maßnahmen zur Wiederherstellung der IT-Security nach IT-Securityvorfällen festzulegen.
- Die Mitarbeiter werden in der Ausführung der Maßnahmen geschult.
- Sofern technisch möglich werden die Maßnahmen trainiert.
- Die Wirksamkeit der Maßnahmen wird regelmäßig im Rahmen des Risikomanagements überprüft.

Hinweise der KAS zu Drohnenangriffen auf Betriebsbereiche nach StörfallV

Grundsätzlich ist von zwei Szenarien auszugehen:

1. Ausspähen eines Betriebsbereichs mit dem Ziel der Planung einer späteren Straftat oder eines späteren Angriffes.

2. Unmittelbarer Angriff einer oder mehrerer Drohnen auf einen Betriebsbereich.

Hinweise der KAS zu Drohnenangriffen auf Betriebsbereiche nach StörfallV

2.1 Grundlegende Maßnahmen

- Der Betreiber des Betriebsbereichs ist dafür verantwortlich das Risiko durch Drohnenangriffe zu bewerten und ggf. notwendige technische und organisatorische Maßnahmen zu ergreifen. Diese Maßnahmen müssen Verhaltensregeln für Beschäftigte beim Erkennen und Bewerten von Drohnenanflügen sowie zur Abwehr von Drohnenangriffen beinhalten.

- Der Betreiber veranlasst die Sensibilisierung seiner Mitarbeiter und ggf. weiterer Personen, die im Betriebsbereich tätig sind, über die Gefahren durch Drohnen. Hierzu können z. B. Schulungen durchgeführt werden, die auf die getroffenen Maßnahmen (passive oder aktive) eingehen und auch das Erkennen von Drohnenangriffen berücksichtigen.

Hinweise der KAS zu Drohnenangriffen auf Betriebsbereiche nach StörfallV

2.2 Passive Maßnahmen

- Passive Maßnahmen sind solche, die präventiv und unabhängig von einem konkreten Drohnenangriff getroffen werden können. Voraussetzung zum Ergreifen von passiven Maßnahmen ist die Ermittlung aller sicherheitsrelevanten Anlagenteile, die durch Drohnen empfindlich gestört werden können und deren Dokumentation.

- Maßnahmen, die einen unmittelbaren Anflug auf sicherheitsrelevante Anlagenteile wirksam verhindern können, sind z. B.
  - Einhausung,
  - Sichtschutz,
  - Schutz von Öffnungen, wie z. B. offenen Fenstern, gegen Durchflug,
  - Schutznetze gegen Anflug auf außen liegende Anlagenteile.

Hinweise der KAS zu Drohnenangriffen auf Betriebsbereiche nach StörfallV

2.3 Aktive Maßnahmen

- Aktive Maßnahmen sind solche, die zum Erkennen und ggf. zur Abwehr eines konkreten Drohnenanflugs getroffen werden.
- Der Betreiber prüft, ob Einrichtungen zum Erkennen von Drohnenanflügen notwendig, verfügbar und geeignet sind.
- Ist ein Erkennungssystem installiert, sind für den Fall des Erkennens eines Drohnenanflugs vom Betreiber organisatorische, z. B. Meldeverfahren, und ggf. technische Maßnahmen zu treffen. Die Beschäftigen sind entsprechend zu unterweisen.
- Die rechtliche Bewertung weiterer aktiver Maßnahmen durch den Betreiber, z. B. Abfangen/Abschuss von Drohnen oder Erzwingen einer geordneten Landung, ist gegenwärtig unklar.

Hinweise der KAS zu Drohnenangriffen auf Betriebsbereiche nach StörfallV

Sachstand zu den aktuellen Arbeiten des KAS zur Problematik „Eingriffe Unbefugter" (Überarbeitung des SFK-GS-38)

- Erster Entwurf der Neufassung des SFK-GS-38 liegt vor und wurde der KAS vorgestellt. Leitsätze zu cyberphysischen Angriffen und Hinweise zu Drohnenangriffen sind implementiert.
- Verabschiedung der Neufassung durch die KAS für Nov. 2019 geplant
- Veröffentlichungstermin: Anfang 2020

Hinweis: Veröffentlichung des Ausschusses für Betriebssicherheit beim BMAS

EmpfBS 1115 (März 2019): Umgang mit Risiken durch Angriffe auf die Cyber-Sicherheit von sicherheitsrelevanten MSR-Einrichtungen (Download über www.baua.de möglich)

25.09.2019

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Prof. Dr. Thomas Schendler
Bundesanstalt für Materialforschung und -prüfung (BAM)
Abteilung „Chemische Sicherheitstechnik“
12205 Berlin, Unter den Eichen 87
Tel.: 030 8104-1200, Email: thomas.schendler@bam.de