# Stellungnahme des TÜV-Verbands zum Referentenentwurf der ersten Verordnung zur Änderung der Bekanntgabeverordnung (41. BImSchV) im Rahmen der Anhörung der beteiligten Kreise nach § 51 BImSchG

## Stand 25. März 2024

Der TÜV-Verband unterstützt die Ergänzung der 41. BImSchV um das Teilfachgebiet „Prozessleittechnik – CyberSecurity (IT/OT)". Das Risiko von Cyberangriffen ist bereits heute ein wichtiger Aspekt für einen sicheren Anlagenbetrieb. Eine weiterhin steigende Bedeutung aufgrund des fortschreitenden technologischen Wandels ist allseitig unbestritten. Betriebsbereiche nach Störfallverordnung sind dabei besonders in den Blick zu nehmen, da hier erfolgreiche Cyberangriffe nicht nur reale Gefahren für Mensch und Umwelt mit sich bringen, sondern auch weitreichende wirtschaftliche Auswirkungen besitzen können. Für Betriebsbereiche nach Störfallverordnung bestehen mit dem Regelwerk KAS 51 bereits inhaltliche Vorgaben für die Implementierung von Maßnahmen der Security. Jedoch besitzen die gültigen Verfahren für die staatliche Zulassung von Sachverständigen noch keinen Nachweis für eine fachliche Eignung für den Bereich der Cybersicherheit. Diese Lücke soll durch die Ergänzung der 41. BImSchV geschlossen werden.

Aus Sicht des TÜV-Verbands beinhaltet der vorliegende Referentenentwurf jedoch noch Regelungen, die eine schnelle und flächendeckende Verfügbarkeit entsprechender Sachverständiger stark erschweren und somit die Handlungsspielräume der zuständigen Aufsichts- und Genehmigungsbehörden in unnötiger Weise einschränken.

Der Referentenentwurf sollte daher wie nachfolgend beschrieben angepasst werden.

## Kernforderungen

1. Die Anerkennung der Fachkunde für das Teilfachgebiet Nummer 10.2 „Prozessleittechnik – CyberSecurity (IT/OT)" muss ergänzend zu der bisherigen Systematik auch ohne anlagenbezogene Fachkunde und Anerkennung möglich sein.
2. Es sollte eine Übergangsfrist für die Zulassung entsprechender Sachverständiger von mindestens 36 Monaten festgeschrieben werden.
3. Perspektivisch sollte an grundlegenden Regelungen gearbeitet werden, die eine rechtsgebietsübergreifende Behandlung des Themas Cybersicherheit durch den Betreiber unterstützen und eine Nutzung von Synergien im Rahmen genehmigungsrechtlicher und behördlicher Verfahren sowie bei rechtsgebietsabhängigen Nachweispflichten vereinfachen.

## 1. Isolierte Fachkunde für das neue Teilfachgebiet Nummer 10.2

Der aktuelle Referentenentwurf sieht die bisher übliche Kopplung der Anerkennung von Fachgebieten mit einer anlagenbezogenen Fachkunde im Sinne von § 7 Nr. 3 und 4 sowie Anlage 2 A auch für das Teilfachgebiet Nummer 10.2 „Prozessleittechnik – CyberSecurity (IT/OT)" vor.

Zutreffend ist, dass für eine abschließende Bewertung der Sicherheit einer Anlage nicht nur eine Bewertung ihrer Verwundbarkeit durch Cyberangriffe erforderlich ist. Es müssen auch Kenntnisse darüber vorhanden sein, welche physischen Auswirkungen aus eingetretenen digitalen Kompromittierungen verfahrenstechnischer Systeme entstehen können. In der Industrie geübte Praxis ist, dass diese erforderliche Gesamtbewertung von der Cyberbedrohung über mögliche Kompromittierungen bis hin zu betrachtenden Störfällen durch interdisziplinäre Teams erarbeitet werden, bei denen Cybersicherheitsexperten mit ausreichenden Erfahrungen im Bereich der sogenannten OT (Operational Technology)-Security mit verfahrens- und anlagentechnischen Spezialisten zusammenarbeiten. Durch dieses Zusammenwirken von qualifizierten Personen wird sichergestellt, dass die Kompetenzen und Erfahrungen der Beteiligten in den sich inhaltlich stark unterscheidenden Fachdisziplinen ein solides Fundament für die erforderlichen Bewertungen bilden. Die gleichwertige Vereinigung entsprechender Kompetenzen, d.h. bezüglich Cybersicherheit und Anlagen- bzw. Verfahrenstechnik, in einer einzigen Person ist bisher nur in sehr wenigen Fällen zu beobachten und wie oben dargestellt auch nicht zwingend erforderlich.

Die im Referentenentwurf enthaltene Kopplung von dem Fachgebiet Cybersicherheit mit anlagenbezogenen Fachkunden wird dazu führen, dass von der gemessen an den Marktbedürfnissen ohnehin schon geringen Anzahl von Sachverständigen im Bereich der IT-/OT-Security für viele Anlagenarten nur ein Bruchteil die Vorgaben für die staatliche Zulassung erfüllen wird. Eine schnelle und flächendeckende Verfügbarkeit entsprechender Sachverständiger kann somit voraussichtlich nicht sichergestellt werden. Das in der Begründung unter „Zielsetzung und Notwendigkeit der Regelungen" beschriebene Ziel der effektiven Unterstützung der Vollzugsbehörden droht deshalb verfehlt zu werden.

Eine höhere Verfügbarkeit von staatlich zugelassenen Sachverständigen bei gleichzeitiger Transparenz hinsichtlich der ausreichenden fachlichen Qualifikation lässt sich dadurch erreichen, die Anerkennung der Fachkunde für das Teilfachgebiet Nummer 10.2 „Prozessleittechnik – CyberSecurity (IT/OT)" ergänzend zu der bisherigen Systematik auch ohne anlagenbezogene Fachkunde zu ermöglichen. Für Sachverständige ohne anlagenbezogene Fachkunde wäre in diesem Fall festzuschreiben, dass eine abschließende sicherheitstechnische Bewertung im Rahmen einer Beauftragung als Sachverständiger nach § 29b BImSchG nur in Zusammenarbeit mit einem Sachverständigen mit anlagenbezogener Fachkunde erfolgen darf. Die Zusammenarbeit von Sachverständigen mit unterschiedlichen Kompetenzfeldern zur Bearbeitung von fachgebietsübergreifenden Fragestellungen oder beim Erfordernis sehr tiefer Spezialkenntnisse ist bereits heute schon üblich und bewährt, auch wenn dies

bisher nicht in der vorgenannten Art durch die 41. BImSchV vorgesehen ist, sondern beispielsweise durch die Nutzung von sogenanntem Hilfspersonal erfolgt.

Gleiches gilt auch für die Anerkennung der Fachkunde nach Nr. 10.1 „MSR-/Prozessleittechnik (OT)".

## 2. Ergänzung einer Übergangsfrist

Der vorliegende Referentenentwurf der 41. BImSchV sieht ein Inkrafttreten ohne Übergangszeit vor, damit Antragstellung, Bekanntgabe und Beauftragung von Sachverständigen im neuen Teilfachgebiet 10.2 unmittelbar erfolgen können.

Hinsichtlich der Antragstellung und Bekanntgabe begrüßen wir dieses Vorgehen, auch wenn uns keine Informationen dazu vorliegen, ob bei den betroffenen Vollzugsbehörden die hierfür erforderlichen fachlichen Vorgaben für die bei der Antragstellung zu erbringenden Kompetenznachweise bereits vorhanden sind. Um dies voranzubringen, steht der TÜV-Verband für Gespräche über die erforderlichen Qualifikationen auf dem Gebiet der Cybersicherheit zu Verfügung.

Hinsichtlich der Beauftragung von Sachverständigen sehen wir erhebliche Risiken für den genehmigungsrechtlichen- und behördlichen Vollzug für den Fall, dass keine Übergangszeit festgelegt wird. Die Berücksichtigung der fachlichen Vorgaben insbesondere des Leitfadens KAS 51 zu Fragen der IT-/OT-Security ist bereits heute schon Bestandteil einer Vielzahl von Prüfungen nach § 29 a BImSchG. Bei Inkrafttreten der Regelungen zum neuen Teilfachgebiet 10.2 wird den Sachverständigen nach § 29 b BImSchG faktisch unmittelbar die Berechtigung entzogen, entsprechende Bewertungen zur Cybersicherheit durchzuführen. Da von einem erheblichen Zeitbedarf für die Erlangung einer Anerkennung für das neue Teilfachgebiet 10.2 auszugehen ist, ständen dann den Vollzugsbehörden für diesen Zeitraum keine anerkannten Sachverständigen mehr zur Verfügung.

Die Antragstellung und Bekanntgabe von Sachverständigen im neuen Teilfachgebiet 10.2 sollte daher unmittelbar nach Verkündung der Verordnung möglich sein, für die Erbringung von entsprechenden Prüfungen nach § 29 a BImSchG sollte eine Übergangszeit für die verpflichtende Beibringung einer Anerkennung für das Teilfachgebiet 10.2 von mindestens 36 Monaten gelten.

Bis zur Bekanntgabe von § 29 b Sachverständigen mit Fachgebiet 10.2 in ausreichender Anzahl, sollten Nebenbestimmungen in Genehmigungsbescheiden bei Prüfungen der Cybersecurity nicht auf dieses Fachgebiet abheben.

## 3. Rechtsgebietsübergreifende Behandlung des Themas Cybersicherheit

Nachweispflichten zur Cybersicherheit halten in berechtigter Weise nach und nach Einzug in nahezu allen Rechtsgebieten, in denen staatliche Vorgaben zum Schutz von Mensch, Umwelt und der öffentlichen Ordnung bestehen. Die Schutzziele, denen die Cybersicherheit dienen soll, unterscheiden sich hierbei genauso wie die Arten der in den jeweiligen Rechtsgebieten etablierten Nachweisführungen.

Die grundlegenden Vorgehensweisen und Prozesse der Cybersicherheit sind hiervon jedoch unberührt. In vielen Fällen wird durch den Betreiber ein geeigneter und alle relevanten Rechtsgebiete abdeckender Ansatz für alle seine Anlagen und Betriebsbereiche verfolgt. Hieraus ergibt sich ein einheitliches Cybersicherheitsregime des Betreibers, auf dessen Basis die effektive Erfüllung seiner rechtlichen Nachweispflichten ermöglicht wird. Somit können durch einen solchen Ansatz Aufwände für die Wirtschaft sowohl für die Implementierung und Aufrechterhaltung als auch für die Nachweispflichten reduziert und der zielgerichtete Einsatz der nur in begrenzter Anzahl vorhandenen Experten gefördert werden. Voraussetzung hierfür ist jedoch die ressortübergreifende Abstimmung der Anforderungen an ein integrales Cybersicherheitsregime für Unternehmen und die Verankerung entsprechender Regelungen in den einzelnen Rechtsgebieten.

Wird dieses Ziel erreicht, entstehen eine Vielzahl von nutzbaren Synergien, die den Abbau von Überlappungen und partiellen Doppelprüfungen im Rahmen der Tätigkeiten von Behörden und Prüforganisationen ermöglichen. Der TÜV-Verband bietet sich als kompetenter Ansprechpartner an, einen solchen Weg konstruktiv zu begleiten.

Als TÜV-Verband e.V. vertreten wir die politischen Interessen der TÜV-Prüforganisationen und fördern den fachlichen Austausch unserer Mitglieder. Wir setzen uns für die technische und digitale Sicherheit sowie die Nachhaltigkeit von Fahrzeugen, Produkten, Anlagen und Dienstleistungen ein. Grundlage dafür sind allgemeingültige Standards, unabhängige Prüfungen und qualifizierte Weiterbildung. Unser Ziel ist es, das hohe Niveau der technischen Sicherheit zu wahren, Vertrauen in die digitale Welt zu schaffen und unsere Lebensgrundlagen zu erhalten. Dafür sind wir im regelmäßigen Austausch mit Politik, Behörden, Medien, Unternehmen und Verbraucher:innen.

Herausgeber
TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095-400
Fax: +49 30 760095-401
E-Mail: berlin@tuev-verband.de
www.tuev-verband.de