

Technische Überwachung

Anlagensicherheit
Arbeits- und Gesundheitsschutz
Umweltschutz



Moderne
Anlagensicherheit:
Innovation und
Regulierung

Künstliche
Intelligenz in der
Anlagensicherheit

Am Anlagensicherheitsreport sind folgende Zugelassene Überwachungsstellen beteiligt



DEKRA Automobil GmbH, DEKRA Testing and Certification GmbH,
GTÜ Anlagensicherheit GmbH,
SGS-TÜV Saar GmbH,
TÜV Austria Services GmbH,
TÜV NORD Systems GmbH & Co. KG,
TÜV Technische Überwachung Hessen GmbH,
TÜV Rheinland Industrie Service GmbH,
TÜV SÜD Chemie Service GmbH, TÜV SÜD Industrie Service GmbH,
TÜV Thüringen e. V.

Editorial 4

Moderne Anlagensicherheit verbindet Innovation und Regulierung 6

Cybersecurity: Schutz mit höchstem Anspruch 9

Komplexität managen: Sicherheit in modernen Anlagen 12

Welche Risiken der Wegfall der Erlaubnispflicht birgt 14

Man muss immer das KI-Gesamtsystem denken 18

Mängelstatistik

Prüfungen von Aufzugsanlagen 23

Prüfungen von Druckanlagen 29

Prüfungen von Ex-Anlagen 36

Adressen der beteiligten ZÜS 55

Bürokratieabbau praxisnah gestalten

Politische
Unsicherheiten
nehmen zu

Die Klimakrise, Digitalisierung und Künstliche Intelligenz sowie zahlreiche politische Krisen in Deutschland, Europa und der Welt bestimmen unsere Zeit. Die Wirtschaft steht unter Anpassungsdruck, Unternehmen finden immer schwerer geeignete Fachkräfte und klagen über zu viel Bürokratie. Die Zugelassenen Überwachungsstellen (ZÜS) begleiten diese Diskussionen konstruktiv und unterstützen alles, was Prüfungen vereinfacht. Wir weisen aber auch auf Probleme hin. Die geplante Abschaffung der Erlaubnispflicht für die Errichtung überwachungsbedürftiger Anlagen würde beispielsweise bedeuten, dass die bisher obligatorische Vorprüfung durch eine ZÜS wegfällt. Im Extremfall kann das dazu führen, dass eine bereits errichtete Anlage wieder zurückgebaut werden muss. Das hilft niemandem, kostet viel Geld und Zeit. Solche Konstellationen sollten vom Gesetzgeber vermieden werden.

Im Bereich der digitalen Sicherheit haben wir es mit einer Reihe zusätzlicher Anforderungen wie der NIS2-Richtlinie zu tun, um ein angemessenes IT-Sicherheitsniveau zu erreichen. Für die Betreiber der Anlagen steigen die zu prüfenden Anforderungen an die Cybersicherheit schrittweise an. Wurden alle sicherheitskritischen Systeme identifiziert? Wurden die richtigen Schutzmaßnahmen gewählt? Gibt es ein Notfallmanagement? Diese und weitere Fragen stellen die Sachverständigen in Zukunft. Das ist notwendig, denn Cyberangriffe auf Unternehmen und kritische Infrastrukturen haben im Zuge der rasanten Entwicklung von Künstlicher Intelligenz und zunehmender internationaler Spannungen noch einmal stark zugenommen. Die Sicherheit digitaler Systeme und KI-Anwendungen muss daher immer Bestandteil

Steigende Anforderungen an die Cybersicherheit

technischer Prüfungen sein: egal ob es sich um vernetzte Anlagen für die Energieerzeugung, der industriellen Produktion oder um digital gesteuerte Aufzüge handelt.

Trotz der aktuell schwierigen wirtschaftlichen Lage dürfen wir die Dekarbonisierung des Energiesektors nicht aus den Augen verlieren. Der Ausbau erneuerbarer Energien und der Aufbau einer Wasserstoffinfrastruktur macht unser Land unabhängiger und wettbewerbsfähiger. Ob Solarfelder, Windparks oder Wasserstoffnetze – die Akzeptanz neuer Energieträger steht und fällt mit ihrer Sicherheit. Die Sachverständigen der ZÜS begleiten mit ihren unabhängigen Prüfungen den Umbau zu einer klimafreundlichen und sicheren Energiewirtschaft. Unser Ziel ist es, den industriellen Kern unseres Landes und die Wettbewerbsfähigkeit Europas zu erhalten.

Ich wünsche Ihnen eine anregende Lektüre!



Dr. Joachim Bühler
Geschäftsführer
TÜV-Verband e. V.

Moderne Anlagensicherheit verbindet Innovation und Regulierung

Von Dieter Roas

Der dynamische technologische Wandel fordert Arbeitgeber, Betreiber, Behörden und zugelassene Überwachungsstellen mehr denn je: Um das hohe Sicherheitsniveau zu halten, gilt es, die Chancen digitaler, vernetzter und KI-basierter Systeme zu nutzen und zugleich deren Risiken im Blick zu behalten. Dafür bietet ein neuer Rechtsrahmen die Möglichkeiten und muss jetzt praxistauglich konkretisiert werden. Entscheidend bleibt die unabhängige Drittprüfung von überwachungsbedürftigen Anlagen, der zugehörigen Daten, IT-Systeme und wo nötig der dahinterliegenden Algorithmen.

Nach dem neuen Gesetz über überwachungsbedürftige Anlagen (ÜAnIG) sollen in den kommenden Monaten die Referentenentwürfe für die Überwachungsbedürftige Anlagenverordnung (ÜAnIV) und zur Arbeitsmittelbenutzungsverordnung (AMBV) erscheinen. Weil einige überwachungsbedürftige Anlagen zugleich als Arbeitsmittel gelten, sind fallweise beide Verordnungen anzuwenden. Beispiel dafür sind Aufzüge für den Materialtransport, Druckbehälter zum Speichern von Gasen oder Dampferzeuger für Produktionsprozesse.

Die beiden Verordnungen müssen so konzipiert werden, dass sie sich ergänzen, aber auch klar voneinander abgegrenzt sind. Das soll doppelte Arbeiten bei der Einhaltung von Vorschriften vermeiden, den bürokratischen Aufwand reduzieren und ein effizienteres und moderneres Sicherheitsmanagement fördern. Während die ÜAnIV das ÜAnIG für die Umsetzung in der Praxis

konkretisiert, wird die geplante AMBV die Arbeitsmittel aus der heutigen Betriebssicherheitsverordnung (BetrSichV) erfassen, die keine überwachungsbedürftigen Anlagen sind.

Beide Verordnungen ersetzen dann die in die Jahre gekommene BetrSichV. Ziel dieser Änderungen muss sein: noch mehr Praxisnähe sowie eine verbesserte Lesbarkeit und Verständlichkeit für Arbeitgeber und Betreiber. Die Prüfunternehmen müssen sowohl die spezifischen Anforderungen der ÜAnIV kennen als auch die umfassenden Anforderungen der AMBV. Nur so können sie eine überwachungsbedürftige Anlage richtig prüfen und eine valide Aussage für die sichere Verwendung bis zur nächsten Prüfung leisten.

Gesetzlicher Rahmen und Hintergrund der Aktualisierung

Nötig geworden ist das neue ÜAnIG auch, weil sich der Rechtsrahmen zu

überwachungsbedürftigen Anlagen seit 1953 kaum verändert hat – die Anlagentechnik dagegen in hohem Maße. Überwachungsbedürftige Anlagen waren zuvor im Produktsicherheitsgesetz (ProdSG) geregelt. Die Auslagerung in ein eigenständiges Gesetz trug sowohl ihrer besonderen wirtschaftlichen Bedeutung Rechnung als auch dem besonderen Gefährdungspotenzial.

Der Gesetzgeber hat zum einen veraltete Formulierungen und strukturelle Mängel aktualisiert und korrigiert. Zum anderen hat er den zugehörigen Text übersichtlicher und zielgerichteter gestaltet. Diese Verbesserungen dürften insbesondere für Betreiber von überwachungsbedürftigen Anlagen zu mehr Klarheit beitragen. Auch wurden die Voraussetzungen für die Anerkennung von Zugelassenen Überwachungsstellen (ZÜS) auf Gesetzesebene transparenter gestaltet. Ein weiteres Ziel ist die „Entbürokratisierung“. Sie ist sinnvoll, birgt aber überall dort Folgerisiken, wo zusätzliche Kontrollinstanzen ein Plus an Sicherheit bedeuten.

Entbürokratisierung und Wegfall der Erlaubnispflicht

Ein Beispiel für das Reduzieren von Kontrollinstanzen ist der geplante Wegfall der Erlaubnispflicht bei bestimmten überwachungsbedürftigen Anlagen. Diese dürfen künftig ohne vorherige Genehmigung durch Behörden errichtet und betrieben werden. Dabei müssen Unternehmen selbst darauf achten, dass ihre Anlagen den geltenden Sicherheitsstandards – und vor allem den erforderlichen Aufstellungsbedingungen – entsprechen, da die behördliche Vorabkontrolle entfällt.

Die Regelung zielt darauf ab, den administrativen Aufwand für Unternehmen zu verringern. Zugleich sollen die Behörden entlastet werden, die personell nicht immer in der Lage sind, alle Genehmigungsanträge zeitnah zu bearbeiten.

Ohne die präventive Überprüfung durch eine Behörde können allerdings potenzielle Sicherheitsrisiken übersehen werden. Der Betrieb einer Anlage kann – insbesondere aufgrund der Umgebungsbedingungen – gefährlich werden. Wird erst nach der Errichtung festgestellt, dass die Anlage zwar sicherheitstechnisch den Anforderungen entspricht, aber am falschen Ort (z. B. mit zu geringen Abständen in einem Wohngebiet) steht, wäre der wirtschaftliche Schaden enorm. Wo die „Verhältnismäßigkeit“ – wirtschaftlicher Schaden vs. sicherer Betrieb (Aufstellungsort) – infrage steht, muss der sichere Betrieb immer Vorrang haben.

Entscheidend ist, dass die Anlagenerichter und -betreiber ihren Sorgfaltpflichten zuverlässig nachkommen und bereits vor der Errichtung nochmals geprüft wird, ob die Aufstellungsbedingungen eingehalten wurden – auch wenn die Behörde dann keine Genehmigung mehr erteilen muss. Hier bestehen noch zahlreiche Herausforderungen, um den Wegfall der Erlaubnispflicht sorgfältig zu gestalten. Das muss auf Fach- und Beratungsgremienebene weiter diskutiert und ausgestaltet werden.

Chancen und Risiken durch neue Technologien

Ein weiterer Hebel zur Steigerung der Effizienz bei der Anlagensicherheit

sind neue Technologien. Kontinuierliche Monitoringsysteme ermöglichen schon heute, Anlagen in Echtzeit zu kontrollieren und auf Basis der erfassten Daten präventiv zu warten und instand zu setzen, bevor es zu Ausfällen und Stillständen kommt. Das erhöht die Produktivität und die Wirtschaftlichkeit des Anlagenbetriebs. Der zunehmende Einsatz von kontinuierlichem Monitoring erleichtert Betreibern auch, ihrer Verpflichtung für einen sicheren Anlagenbetrieb nachzukommen. Nun gilt es, klare Regelungen zu schaffen, um eine geeignete Berücksichtigung dieser Technologie bei ZÜS-Prüfungen zu ermöglichen. Alle Prüforganisationen leisten hohe Aufwände bei der Aus- und Weiterbildung, um beim Fachwissen auf Augenhöhe mit dem Betreiber oder Hersteller zu sein und die Technologien und ihre Auswirkungen auf die Sicherheit bewerten zu können.

Ob eine fallweise geforderte risikobasierte Inspektion (RBI) geeignet ist, die heute bewährten Prüfintervalle und Prüftiefen beliebig zu verändern, muss sehr genau betrachtet werden, um unser hohes Sicherheitsniveau in Deutschland nicht infrage zu stellen. Die Anlagensicherheit darf nicht zu einer Black Box oder auf ein intransparentes Unterfangen unterschiedlicher Interessen reduziert werden.

KI verändert Anlagenbetrieb und -prüfung

KI ermöglicht zunehmend, Anlagen näher an den Auslegungsgrenzen und damit wirtschaftlicher zu betreiben. Und sie hat auch für die Anlagensicherheit das Potenzial, Prüfprozesse zu optimieren und die umfangreichen Anlagendaten schneller und in der

Tiefe zu analysieren. Das kann dazu beitragen, Ausfälle zu minimieren, die Sicherheit der Anlagen zu erhöhen und die Genauigkeit und Zuverlässigkeit von Gefährdungsbeurteilungen zu verbessern bzw. zielgerichteter zu bewerten. Wichtig dabei ist, KI nicht isoliert zu betrachten. Sie ist Teil eines umfassenden Sicherheitssystems, das menschliche Überwachung und automatisierte Prozesse umfasst. Als Werkzeug müssen KI und ihr Einsatz selbst ständig überprüft und optimiert werden – aber auch reguliert. Hier hat die EU mit der risikobasierten KI-Verordnung einen sinnvollen Ansatz gefunden: Je höher das Gefährdungspotenzial, desto umfangreicher müssen die regulatorischen Anforderungen sein.

Eine mögliche Integration von KI in sicherheitsrelevante Systeme wirft nicht nur regulatorische und rechtliche, sondern auch technische und ethische Fragen auf. Die Verantwortung für und die Transparenz von KI-Entscheidungen sind hier besonders relevant. Sachverständige müssen jederzeit Zugriff auf die Daten und im Bedarfsfall auf die zugehörigen Algorithmen haben. Wo KI-Systeme auf internationalen Servern und internationalem Recht aufbauen, dürfte das den nach nationalem Recht agierenden ZÜS und Behörden die Arbeit erschweren. Hier gilt es, vorab die Befugnisse, die Sanktionsmöglichkeiten sowie etwaige Abhängigkeiten zu klären.

Unabhängige Prüfung als Basis von Innovationen

Es gibt immer wieder die Annahme, dass eine Regulierung die Integration von Innovationen bremst. Es ist aber vielmehr so, dass Regulierung eine

Grundbedingung für deren Integration und nicht zuletzt für das Vertrauen in innovative Technologien ist. Denn es gibt keine nachhaltigen Märkte ohne Regeln. Und Innovationen werden nur in geregelten Systemen sicher und wirtschaftlich nutzbar.

Und hier ist die unabhängige Prüfung ein zentraler Stützpfiler, um Innovationen in überwachungsbedürftige Anlagen zu integrieren. Denn nur sie ermöglicht, dass die Gesamtsysteme sicher bleiben, die Betreiber ihrer Verantwortung gerecht werden können und Vertrauen gegenüber der Bevölkerung aufgebaut wird. Insbesondere in sicherheitskritischen Bereichen ist es unerlässlich, dass Entscheidungen, die von KI-Systemen getroffen werden, von qualifizierten Fachleuten nachvollzogen und gegebenenfalls korrigiert werden können. Die Rolle der unabhängigen Prüfung entwickelt sich somit weiter und umfasst künftig immer mehr die Prüfung und die Bewertung der datengesteuerten Prozesse und der Algorithmen, die in den Anlagen eingesetzt werden.

Um mit hochdynamischen Entwicklungen Schritt zu halten, gilt es, die Prüfstandards und -regeln ständig zu aktualisieren und schneller anzupassen. Sachverständige müssen durch Schulungen gewährleisten, dass sie sowohl mit bisherigen Verfahren als auch mit innovativen Systemen arbeiten können. Darüber hinaus muss eine kontinuierliche Weiterbildung auf hohem Niveau sichergestellt sein. So trägt die unabhängige Prüfung auch künftig effektiv dazu bei, Gefährdungen zu minimieren und die Sicherheit, Umweltverträglichkeit und Verfügbarkeit überwachungsbe-

dürftiger Anlagen weiterhin sicherzustellen.

Unser hoher Sicherheitsstandard, den wir heute bei überwachungsbedürftigen Anlagen haben, basiert nicht zuletzt auf dem Zusammenwirken von Betreibern, Wartungs- und Instandhaltungsunternehmen, Behörden und der unabhängigen Drittprüfung. Und es ist eine gemeinsame Verantwortung, das hohe Sicherheitsniveau weiter aufrechtzuerhalten. Dafür gilt es, technische Innovationen proaktiv, aber verantwortungsbewusst umzusetzen und zugleich wirksam und dynamisch zu regulieren.



Dieter Roas, Vorsitzender des Erfahrungsaustauschkreises der Zugelassenen Überwachungsstellen und Leiter Geschäftsfeld Fördertechnik TÜV SÜD Industrie Service

dieter.roas@tuvsud.com



Cybersicherheit

Schutz mit höchstem Anspruch

Cyberkriminelle gehen immer professioneller und breiträumiger bei ihren Attacken auf Unternehmen vor. Betreiber überwachungsbedürftiger Anlagen müssen sich besonders schützen – auch wegen erhöhter gesetzlicher Anforderungen. Zugelassene Überwachungsstellen (ZÜS) überprüfen, ob die notwendigen Sicherheitsvorkehrungen umgesetzt wurden.

Erst legt ein eingeschleustes Schadprogramm den Betrieb lahm. Dann melden sich die Cyberkriminellen und verlangen ein Lösegeld für das Freischalten der IT-Systeme. Immer mehr Unternehmen werden Opfer solcher Erpressungsversuche. Es stünden nicht mehr nur „große, zahlungskräftige Unternehmen im Mittelpunkt der Attacken“, heißt es im jüngsten Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI). Zunehmend würden auch kleine und mittlere Firmen angegriffen. Dabei gehen die Cyberkriminellen laut BSI immer perfider vor – als „Cybercrime-as-a-Service“ beschreiben die Sicherheitsexperten die zunehmende Professionalisierung und Spezialisierung der Online-Kriminellen. Mithilfe von Künstlicher Intelligenz gelingt es ihnen, ihre Phishing-Mails immer glaubwürdiger zu gestalten und noch gefährlichere Viren zu programmieren.

Mehr Widerstandskraft gegen solche Cyberangriffe sollen neue Gesetze bringen. So ist beispielsweise in der Europäischen Union (EU) im vergangenen Jahr die NIS2-Richtlinie in Kraft getreten. Sie verpflichtet die Betreiber von kritischer Infrastruktur (KRITIS) – etwa Energieversorger und medizinische Einrichtungen – zu umfassenderen Vorkehrungen für die IT-Sicherheit. „Die Vorgaben für KRITIS-Betreiber wurden massiv verschärft“, sagt Jörg Becker, Leiter des Kompetenzzentrums Cybersecurity der TÜV SÜD Industrie Service GmbH. In Deutschland müssten rund 30.000 Unternehmen künftig die Anforderungen des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes der Bundesregierung erfüllen. Viele von ihnen seien zugleich auch Betreiber überwachungsbedürftiger Anlagen, erläutert Becker. Auch als solche müssen sie strengen regulatorischen

Auflagen gerecht werden. Dieses schlägt sich auch in zunehmenden Prüfumfängen der ZÜS nieder.

Den Unternehmen ist die Notwendigkeit von Cybersecurity bewusst

Das Bewusstsein für Cybergefahren sei in den Unternehmen deutlich gestiegen, sagt Becker. „Wir diskutieren mit den Firmen meist nicht mehr darüber, ob man Cybersecurity braucht – das ist eine gute Nachricht. Aber es schließt sich häufig die Frage an: Was müssen wir tun?“ Vielen Verantwortlichen sei noch nicht klar, wie sie mit den gesetzlichen Vorgaben umzugehen haben. Immer wieder werde zudem der Aufwand unterschätzt. „Man wiegt sich in vermeintlicher Sicherheit, weil man glaubt, dass die Firmen-IT sich um das Thema gekümmert hat“, sagt Becker, „aber die IT-Leute schauen sich nicht unbedingt OT-Systeme an.“ OT steht für Operational Technology. „Bei der OT spielt aber meist die Musik, wenn es um die Sicherheit von Menschen geht“, sagt Becker.

Den Zugriff auf die Anlagen erlangen Cyberkriminelle laut einer BSI-Studie am häufigsten über mit Viren infizierte USB-Sticks oder temporäre Datenverbindungen etwa über verseuchte Wartungsrechner. Werden diese mit einem industriellen Steuerungssystem verbunden, können Hacker die Kontrolle über die Anlagen übernehmen. „Mitarbeiter werden so unwissend zu Tätern, weil sie mit kompromittierten Werkzeugen arbeiten“, sagt Becker. Deshalb müsse jede mögliche Verbindung zur Anlagensteuerung beim IT-Sicherheitskonzept berücksichtigt werden. „Wer nur Internetverbindungen betrachtet, springt viel zu kurz.“

Cybersicherheit als Prozess

In der Praxis hält Becker ein schrittweises Vorgehen für sinnvoll. „Cybersicherheit ist immer das Ergebnis eines Prozesses“, sagt der TÜV-Experte. „Zuerst gilt es, die für den sicheren Betrieb hinsichtlich der Cybersicherheit relevanten Systeme zu identifizieren – und das zunächst ohne Berücksichtigung von vorhandenen oder geplanten Security-Maßnahmen. Im zweiten Schritt gelte es dann zu prüfen, welche Folgen es haben könnten, wenn die identifizierten Systeme kompromittiert werden – und welche Wege es hierfür für Angreifer gibt. „Das geschieht klassisch in einer Bedrohungs- und Auswirkungsanalyse“, erklärt Becker. „Auf diese Weise wird der Schutzbedarf festgelegt.“

Erst im nächsten Schritt gelte es, „die konkreten Maßnahmen zu wählen, die ein Unternehmen braucht, um den Schutz des Systems zu erreichen.“ Das Problem sei dabei nicht das Fehlen von Lösungen. „Das Problem ist häufig, dass die Unternehmen nicht genau sagen können, was in welchem Umfang geschützt werden muss und was hierfür die besten Mittel sind.“ Bei überwachungsbedürftigen Anlagen sei das Ziel klar, sagt Becker. Die rechtliche Vorgabe laute: Es darf für Beschäftigte und andere Personen nicht gefährlich werden. „Hier betrifft Cybersecurity zwar nur einen kleinen Bereich der Anlage, dafür aber spielt man dort automatisch in der Champions League.“

Technische Regeln geben Sicherheit

Orientieren können sich die Verantwortlichen in den Betrieben bei der Suche nach geeigneten Cyberschutz-

maßnahmen laut Becker am besten an dem Abschnitt 4.5.2 (2) der Technischen Regel für Betriebssicherheit (TRBS) 1115 Teil 1. Hier sind sechs fundamentale Themen der Cybersicherheit aufgeführt: von Segmentierung und Fernzugriff über den Zugangs- und Zugriffsschutz und die Unabhängigkeit von sicherheitsrelevanten Mess-, Steuer- und Regelungseinrichtungen bis hin zur Überwachung sowie dem Notfallmanagement. Auch die „Härtung von Komponenten“ zählt dazu – Soft- und Hardware werden, im Rahmen ihrer bereits vorhandenen Möglichkeiten, möglichst widerstandsfähig aufgestellt. „Ein Unternehmen muss sich für jeden dieser Bereiche überlegen, was es an Maßnahmen braucht“, sagt Becker. „Es ist beispielsweise ein Unterschied, ob eine Anlage auf einem geschützten Werksgelände steht oder ob es sich um eine öffentlich zugängliche Tankstelle handelt.“

Die ZÜS prüfen dann, ob die Maßnahmen dafür geeignet sind, die Anlagen entsprechend den Vorgaben zu schützen. „Diese Bewertung ist nur möglich, indem die ZÜS den Prozess nachvollzieht“, sagt Becker. Unterstützung liefert den Unternehmen der Beschluss B-002 des ZÜS-Erfahrungsaustauschkreises (EK ZÜS). Dieser umfasst auch eine Arbeitshilfe für die Betreiber überwachungsbedürftiger Anlagen. „Das ist ein bisschen wie in der Schule: Man sagt, man lernt fürs Leben – und am Ende fragen doch alle: Was kommt in der Prüfung dran und wie bereite ich mich darauf vor?“, sagt Becker. „Und genau diese Fragen beantwortet die Arbeitshilfe.“

Start mit geringer Prüftiefe

Im vergangenen Jahr sind die ZÜS mit einer geringen Prüftiefe gestartet. „Die Frage war zunächst, ob es eine dokumentierte Behandlung des Cybersicherheitsprozesses gibt“, erläutert Becker. Es sei darum gegangen, gerade kleinere Firmen nicht zu überfordern. „Viele hatten das damals noch gar nicht auf dem Schirm“, so der TÜV-Experte. Waren nicht einmal die grundlegenden Schritte gemacht, wurde ein geringfügiger Mangel festgestellt, für dessen Behebung den Unternehmen per Gesetz ein Jahr Zeit gewährt wird. Seit dem 1. April 2024 ist eine weiter-

gehende Dokumentationsprüfung der Cybersicherheit gemäß dem EK-ZÜS-Beschluss B-002 verpflichtend. Diese auch als Stufe 2 bezeichnete ZÜS-Prüfung ist in vier Schritte unterteilt: Die Experten schauen, ob die richtigen Systeme identifiziert wurden, ob der Schutzbedarf korrekt festgestellt und die richtigen Maßnahmen ausgewählt wurden. Zudem wird ermittelt, ob es Maßnahmen gibt, um das implementierte Cybersicherheitsniveau aufrecht zu erhalten. Das geschieht nach dem Prinzip der Plausibilitätsprüfung. „Wir schauen, ob alles mit Kompetenz und ausreichender Genauigkeit durch-

geführt wurde – und die Ergebnisse entsprechend nachvollziehbar sind.“ Noch nicht terminiert ist die sogenannte Stufe 3, in der auch die technische Umsetzung der Cybersicherheit an den Anlagen selbst geprüft werden muss. Jörg Becker: „Die konkrete Umsetzung von Maßnahmen zu prüfen, bei denen noch nicht festgestellt wurde, ob sie überhaupt geeignet sind, erzeugt nur eine Scheinsicherheit.“

INFO

Wie sich Aufzüge vor Cyberangriffen schützen lassen

Es sollte die gewohnte morgendliche Fahrt ins Erdgeschoss werden. Doch der Aufzug des Wohnhauses bewegte sich immer wieder auf und ab, ohne die Türen zu öffnen. Ende vergangenen Jahres war ein Münchner Familienvater mit seinem einjährigen Sohn in der Anlage gefangen. Erst die Feuerwehr konnte die Fahrt stoppen und die beiden befreien. Die Ursache ist unklar. Es können defekte Steuerungen sein, die Aufzüge aus dem Rhythmus bringen. Doch auch kriminelle Hacker sind in der Lage, die Anlagen zu manipulieren. „Wir nehmen wahr, dass es bei Cyberangriffen in Unternehmen auch Fälle gibt, in denen die Aufzüge betroffen waren“, sagt Guido Kehmer, Geschäftsfeldmanager für Aufzüge und Fördertechnik des TÜV Rheinland. Möglich wird das durch eine zunehmende Vernetzung der Anlagen. „Die Notrufeinrichtung funktioniert

vielerorts über das Internet“, erläutert Kehmer. „Zudem sind Aufzüge in vielen Bereichen mit der Gebäudeleittechnik verbunden.“ Das trifft laut dem Experten auf Kliniken oder Einkaufszentren zu. Zusätzlich können über Internet-of-Things-Anwendungen der Aufzugshersteller Daten des Aufzugs analysiert und abgerufen werden. Häufig vernachlässigte Angriffspunkte sind die Schnittstellen eines Aufzugs, über die beispielsweise drahtgebunden, per WLAN oder Bluetooth die Steuerung erreicht und kompromittiert werden kann. Ob ein technischer Defekt oder ein Cyberangriff die Störung eines Aufzugs verursacht habe, sei nicht immer nachvollziehbar, erläutert TÜV-Experte Kehmer. „Es lässt sich oftmals feststellen, dass Parameter verändert worden sind – aber die Ursache kann häufig nicht zuverlässig ermittelt werden.“

Nicht nur für die Betreiber kritischer Infrastrukturen, sondern für jeden Betreiber einer Aufzugsanlage sei es notwendig, alle Gefährdungen einschließlich der Cybersicherheit zu identifizieren und mögliche Auswirkungen abzuschätzen – um dann geeignete Schutzmaßnahmen zu ergreifen, sagt Kehmer. Diese Schutzmaßnahmen sollten durch eine Gefährdungsbeurteilung für den Aufzug dokumentiert werden. „Die Bauteile eines modernen Aufzugs werden immer elektronischer – und damit auch anfälliger“, erläutert Kehmer. Dass Cyberkriminelle einen Aufzug zum Absturz bringen können, hält der TÜV-Experte für nahezu ausgeschlossen. „Es gibt mechanische Sicherungssysteme, die regelmäßig durch die Zugelassene Überwachungsstelle geprüft werden und im Fall der Fälle dann auch greifen.“

Schutz durch Vernetzung

Komplexität managen: Sicherheit in modernen Anlagen

In überwachungsbedürftigen Anlagen ist neben dem Management der funktionalen Sicherheit die Cybersecurity von entscheidender Bedeutung. Die wachsende technische Komplexität und die zunehmende Vernetzung der Anlagen sind dabei eine enorme Herausforderung. Gefragt ist hier ein ganzheitliches Management, das beide Sicherheitsdisziplinen gleichermaßen im Fokus hat.

Bei der Automatisierung von Prozessen kommen immer mehr vernetzte Geräte und Systeme zum Einsatz und ermöglichen eine präzisere Steuerung von Anlagen sowie die Verarbeitung und Analyse großer Datenmengen. Mit der zunehmenden Verbreitung und Vernetzung computergesteuerter Elemente steigt auch das Risiko, dass deren fehlerhaftes Arbeiten oder Ausfallen schwerwiegende Folgen haben kann. Mögliche Worst-Case-Szenarien durch technisches Versagen sind beispielsweise auftretende Sicherheitsrisiken für Menschen, Umwelt, Anlagen und Prozesse sowie Produktionsausfälle oder die Gefährdung der Cybersicherheit. Besonders dort, wo die Funktionssicherheit von sicherheitsrelevanten Mess-, Steuer- und Regeleinrichtungen von Bedeutung ist, müssen Hersteller und Betreiber Maßnahmen implementieren, um Störungen und Ausfälle zuverlässig zu verhindern. So müssen beispielsweise Sicherheitsventile- und -klappen nicht nur im Normalbetrieb, sondern insbesondere im Notfall zuverlässig arbeiten. Maßnahmen, die dies gewährleisten, sind beispielsweise die Analyse und das angemessene Management des Risikos, eine Architektur mit redundanten Sicherheitsmechanismen, Back-up-Systeme, Tests und Vali-

dierungen in regelmäßigen Intervallen sowie präventive Wartung.

Management der funktionalen Sicherheit ist das A und O

Elektrische, elektronische oder programmierbare elektronische (E/E/PE) Komponenten sind heute zunehmend im Einsatz, wenn es darum geht, die Sicherheit überwachungsbedürftiger Anlagen zu gewährleisten. Zu Störungen kann es dabei vor allem aufgrund systematischer Fehler kommen. Die zugehörigen Normen fordern daher die Implementierung eines Functional Safety Management Systems (FSMS), das solche Fehler verhindern soll. Maßgebliche Grundlagen sind hier, neben der übergeordneten DIN EN 61508, auch die branchenspezifischen DIN EN 61511 und VDI/VDE 2180 (Prozessindustrie) sowie DIN EN 62061 und DIN EN ISO 13849 (Sicherheit von Maschinen).

Das Management der funktionalen Sicherheit umfasst den gesamten Lebenszyklus sicherheitsgerichteter Systeme – von der Konzeption und Bewertung über die kontinuierliche Optimierung bis hin zur Außerbetriebnahme. „Um eine effektive Integration der funktionalen Sicherheit in die

Managementprozesse zu gewährleisten, sollten Betreiber bewährte Maßnahmen ergreifen“, erklärt Markus Pflüger, Geschäftsführer TÜV AUSTRIA Deutschland GmbH und Mitglied des Erfahrungsaustauschkreises der Zugelassenen Überwachungsstellen (EK ZÜS). „Dazu gehören beispielsweise regelmäßige Risikoanalysen, das Befolgen von Branchenstandards und -richtlinien, das Implementieren von Redundanzen, Fehlererkennung und Zugriffskontrollen. Das Sicherheitsbewusstsein sollte durch kontinuierliche Schulungen gefördert und eine Sicherheitskultur im Unternehmen geschaffen werden. Darüber hinaus sollte die Effektivität dieser Sicherheitsmaßnahmen durch regelmäßige Prüfungen und Audits sichergestellt werden.“ Tim Reitzle, Sachverständiger GTÜ sowie Mitglied der ad hoc AG Cybersicherheit des EK ZÜS ergänzt: „Der Betreiber kann Prozesse definieren, um den Anforderungen der funktionalen Sicherheit gerecht zu werden und sie optimal in sein Management zu integrieren. Dazu gehören zum Beispiel Auswahlkriterien für Bauteile bei Neuanlagen oder Umbauten, aber auch Prozesse, die eine Wartung und Prüfung der Komponenten während des Betriebs vorsehen.“

Cybersecurity vs. physische Funktionalität?

Im Zeichen der fortschreitenden Digitalisierung und Industrie 4.0 sind heute mehr und mehr Anlagen vernetzt und erlauben die Fernwartung, Steuerung und Überwachung via Remote-Zugriff. Damit steigt die Gefahr, dass unautorisierte Dritte Zugang zu kritischen Infrastrukturen erhalten. So rückt als zusätzlicher Sicherheitsaspekt neben der funktionalen auch die Cybersicher-

heit verstärkt in den Fokus. Entsprechend fordert die 2023 veröffentlichte Technische Regel für Betriebssicherheit (TRBS) 1115 Teil 1, dass zumindest sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen) vor Cyberangriffen zu schützen sind, wenn sie über Datenschnittstellen verfügen und in der Lage sind, vernetzt zu kommunizieren. Ebenfalls relevant im Hinblick auf die Cybersecurity sind die ISO-27000er-Reihe sowie die IEC 62443er-Reihe. Die ISO 27001 steht dabei für klassische IT-Security, unabhängig von der Branche und der Größe des Unternehmens. Sie definiert, was bei der Implementierung, Überwachung und Pflege eines Informationssicherheitsmanagementsystems (ISMS) zu beachten ist. Die IEC 62443 ist für Hersteller, Betreiber sowie Integratoren von industriellen Automatisierungs- und Steuerungssystemen relevant.

Um überwachungsbedürftige Anlagen effektiv zu schützen, ist ein optimales Zusammenspiel von physischer Funktionalität und diesen Anforderungen an Cybersecurity entscheidend. Bei der Umsetzung stehen jedoch teilweise widersprüchliche Intentionen im Fokus. So gilt es bei der physikalischen Sicherheit beispielsweise den Remote-Zugriff auf Sicherheitssysteme zu ermöglichen, um eine effiziente Steuerung, Überwachung und Fernwartung zu gewährleisten. Unter dem Aspekt größtmöglicher Cybersecurity hingegen wäre es sinnvoll, den Zugang zu den IT-Systemen weitestgehend zu beschränken.

Regelwerke und Maßnahmen dynamisch anpassen

Diese zum Teil gegensätzlichen Ziele beim Management der funktionalen

Sicherheit und der Cybersecurity gilt es, künftig optimal miteinander zu verbinden. „Durch die immer stärker werdende Implementierung von programmierbaren Steuerungen werden neue Angriffsflächen für Sabotage durch Cyberangriffe geschaffen. Diese relativ neue Herausforderung ist aktuell bei Herstellern, Betreibern und bei Prüfern aller Rechtsgebiete ein Thema mit hoher Relevanz“, unterstreicht Tim Reitzle. Und Markus Pflüger erklärt: „Die Systeme werden durch die voranschreitende Digitalisierung und die Einbindung von Künstlicher Intelligenz (KI) in verschiedenen Industriezweigen zunehmend komplexer und miteinander verbunden. Diese wachsende Komplexität von Systemen und Technologien ist aus meiner Sicht künftig die größte Herausforderung im Management der funktionalen Sicherheit.“

Um diesen Herausforderungen gerecht zu werden, sollte ein ganzheitliches Management funktionale Sicherheit und Cybersecurity immer gemeinsam im Blick haben. Zugleich ist es entscheidend, dass Regelwerke und Maßnahmen mit der hohen Dynamik in der Digitalisierung schritthalten und beständig an die neue Entwicklung angepasst werden. Angesichts der wachsenden Komplexität der Technik wie auch der Regelwerke kommt der Prüfung durch unabhängige Stellen eine immer größere Bedeutung zu. Sachverständige und Zugelassene Überwachungsstellen sind durch beständige fachliche Weiterbildung und das Anpassen von Prüfleistungen in besonderem Maße gefordert.

Sicherheitsnetz adé?

Welche Risiken der Wegfall der Erlaubnispflicht birgt

Bürokratie gilt als Wachstums-
hemmnis. Dem will der Gesetzgeber
mit der geplanten Verordnung für
überwachungsbedürftige Anlagen
(ÜAnIV) entgegenwirken. So sollen
Anlagenbetreiber durch den geplanten
Wegfall der Erlaubnispflicht Aufwände
für Genehmigungen und Prüfungen
einsparen. Die Prüforganisationen
begleiten diesen Prozess, um das
hohe Sicherheitsniveau zu erhalten.
Betreiber können jetzt schon
Prüfungen vereinfachen und Doku-
mentationen reduzieren.

Mit der Betriebssicherheitsverord-
nung (BetrSichV) hat der Gesetzge-
ber bereits bürokratische Hürden
abgebaut und beispielsweise die
Anforderungen an die Dokumentation
für Anlagenbetreiber reduziert. Mit
den geplanten Referentenentwürfen
für die Überwachungsbedürftige
Anlagenverordnung (ÜAnIV) und zur
Arbeitsmittelbenutzungsverordnung
(AMBV) besteht ein weiteres Mal die
Möglichkeit, Doppelregelungen zu
vermeiden und die Umsetzung des Ge-
setzes zu Überwachungsbedürftigen
Anlagen (ÜAnIG) unbürokratisch und
praxistauglich auszugestalten. Dabei
gilt es auch, die Verhältnismäßigkeit
im Blick zu behalten.

Die geplante Verordnung für Über-
wachungsbedürftige Anlagen
(ÜAnIG) wird voraussichtlich die
Erlaubnispflicht für bestimmte
überwachungsbedürftige Anlagen

abschaffen. Betreiber solcher Anlagen
benötigen bisher eine behördliche
„Genehmigung“, bevor sie diese
errichten dürfen. Erteilt wird die
Erlaubnis nach erfolgter Prüfung der
Planungsunterlagen und der Aufstel-
lungsbedingungen durch eine Zuge-
lassene Überwachungsstelle (ZÜS).
Betroffene kritisierten diesen bislang
verpflichtenden Schritt als unnötige
Verzögerung.

Der Entfall des Erlaubnisverfahrens
bedeutet für Betreiber aber nicht nur,
dass ein genehmigungsrechtlicher
Schritt und die damit verbundene Do-
kumentation entfallen und damit die
anschließende Bearbeitungszeit von
bis zu drei Monaten eingespart wird.
Auch die Vorprüfung durch eine ZÜS
würde nicht mehr stattfinden. „Sie
ist aber schon eine erste Sicherheits-
prüfung. Ein wichtiger Aspekt sind
dabei die individuell zu bewertenden



Anforderungen an die Aufstell- und Umgebungsbedingungen“, sagt Thomas Prager, Sachverständiger und Leiter der ZÜS für Druckanlagen beim TÜV Rheinland Industrie Service GmbH.

Prüforganisationen sorgen auch für Rechtssicherheit

Im Extremfall stellt eine ZÜS fest, dass die Anlage an ihrem Standort gar nicht hätte errichtet werden dürfen. Ein Wegfall der Erlaubnispflicht ginge daher mit einem erhöhten Risiko einher, dass eine Anlage unter Umständen sogar rückgebaut werden muss. „Die Erlaubnis durch die Behörde bedeutet für den Betreiber auch, dass sich aus nachgelagerten Verfahren wie der Prüfung vor Inbetriebnahme keine grundsätzlichen Probleme aufgrund grober Fehlplanungen ergeben. Wenn künftig die Prüfung vor Inbetriebnahme die erste Prüfung durch

Sachverständige ist, verlieren die Betreiber und Investoren damit auch eine gewisse Rechtssicherheit“, stellt Prager fest. Im Gegensatz dazu hilft eine Prüfung einer Druckanlage im Planungsstadium, frühzeitig Fehler zu vermeiden, die später nur mit großem Aufwand behoben werden können. Hier wird auch das Konzept des Anlagenbetriebs bereits im Vorfeld geprüft. Wechselwirkungen mit benachbarten Anlagen, die möglicherweise nicht in der Verantwortung des antragstellenden Betreibers liegen, werden einbezogen. Das bedeutet mehr Sicherheit für den Menschen, die Umwelt und für Sachwerte – aber auch für Investitionen und geplante Produktionsvolumina.

Thomas Prager fordert daher, „den Prozess der Erlaubnis nicht ersatzlos zu streichen. Ein sinnvoller Ersatz wäre, eine rechtliche Grundlage für

eine alternative unabhängige und planungsbegleitende Vorprüfung durch die ZÜS zu schaffen.“ Vorprüfungen könnten so umgestaltet werden, dass sie bereits in der Planungsphase anhand von Teilprüfungen je nach Prozessschritt vorgenommen würden. Eine solche begleitende Prüfung wäre auch zeiteffizient. Das ist besonders sinnvoll bei Anlagen, bei denen die Aufstellbedingungen eine besondere Rolle spielen. Beispiele dafür sind Tankstellen und Gasfüllanlagen im öffentlichen Raum, aber auch Druckanlagen mit erhöhtem Gefährdungspotenzial wie Dampfkesselanlagen. Das setzt eine gute Abstimmung und das gleiche Grundverständnis für den Vorprüfprozess von Betreiber und ZÜS voraus.

Aufwände eigenverantwortlich reduzieren

Der ersatzlose Wegfall der Erlaubnispflicht wäre deshalb kein sinnvoller

Schritt, um bürokratische Hemmnisse abzubauen, weil er mehr Folgerisiken als Nutzen für die Betreiber birgt. Bis die neue Verordnung – voraussichtlich 2025 – kommt, haben Betreiber jedoch auch nach den bestehenden Vorschriften zahlreiche Möglichkeiten, Erlaubnisverfahren und Prüfungen gegenüber den Standardvorgaben einfacher und effizienter zu gestalten – auch bei der Dokumentation.

Der von Betreiberseite teils kritisierte hohe Dokumentationsaufwand ergibt sich aus verschiedenen Rechtsvorschriften und dem Prinzip der Eigenverantwortung, das in der BetrSichV verankert ist. Danach müssen Betreiber selbst eine Gefährdungsbeurteilung erstellen. Sie müssen also in jedem Einzelfall mögliche Gefährdungen ermitteln, die angemessenen Schutzmaßnahmen festlegen und alles dokumentieren. Das bedeutet auch Freiheiten. Maßgeschneiderte Schutzmaßnahmen führen nicht nur zu mehr Sicherheit, sondern überdies zu weniger Betriebsunterbrechungen.

Um diese Maßnahmen zu entwickeln, sind ausreichend qualifizierte Fachkräfte nötig. Hier gibt Jörg Schöpe vom TÜV Thüringen zu bedenken, „dass die Vielzahl der deutschen Unternehmen klein- und mittelständisch geprägt ist. Sie haben oft kein eigenständiges Engineering und benötigen Unterstützung durch klare und sicherheitstechnisch sinnvolle rechtliche Regelungen. Mit klaren Anforderungen für einen Anlagentyp könnte eine künftige ÜAnIV solche Unternehmen entlasten. Ein reiner gefährdungsbezogener Ansatz hingegen mit einer Vielzahl an Dokumentationspflichten durch den Betreiber fordert diese heraus. Denn um durch eine sinnvoll strukturierte

Gefährdungsbeurteilung Aufwände eigenverantwortlich reduzieren zu können, ist ein hohes Maß an Erfahrung und Fachwissen nötig.“ So kann beispielsweise eine mögliche Mehrfachdokumentation vermieden werden, wenn ähnliche und verwandte Tätigkeiten auch als solche betrachtet werden. Abhängig von der Gefährdung lassen sich allgemeingültige Schutzmaßnahmen festlegen, die dann unter Umständen für einzelne Arbeitsmittel nur noch spezifisch ergänzt werden. Die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, BAuA, liefert praktische Anleitungen, beispielsweise nachzulesen im „Handbuch Gefährdungsbeurteilung“.

Effizienter mit individuellen Prüfkonzepthen

Auch mit sogenannten Prüfkonzepthen ermöglicht die BetrSichV, wiederkehrende Prüfungen abweichend von den Standardabläufen zu gestalten. Dazu regelt Anhang 2, Abschnitt 4 Nr. 5.7 BetrSichV Ersatzprüfungen, die durchgeführt werden können für

- > die Besichtigung drucktragender Wandungen bei der wiederkehrenden inneren Prüfung und
- > die statische Flüssigkeitsdruckprüfung bei der wiederkehrenden Festigkeitsprüfung.

Ein Prüfkonzepth nach BetrSichV ist ein systematischer Plan, der die Prüfungen an Anlagenteilen von überwachungsbedürftigen Druckanlagen für eine Prüfaussage zum sicheren Betrieb festlegt. Dies umfasst sowohl die Art der Prüfung (z. B. Sichtprüfungen, zerstörungsfreie Prüfungen zFP, Wasserdruckprüfungen) als auch die Festlegung der Prüffristen und die

Qualifikation der Prüfenden. Es können dabei auch Maßnahmen festgelegt werden, bei deren Anwendung die Druckanlage oder Anlagenteile nicht außer Betrieb genommen werden müssen.

Betreiber können Prüfkonzepthe selbst erstellen oder ein fertiges Konzept aus nichtstaatlichen technischen Regeln auswählen, das für ihre Anlage geeignet ist. Das Konzept muss lediglich durch eine ZÜS bestätigt werden – bedarf jedoch keiner Behördenbeteiligung.

Ein ähnliches Beispiel ist die Einführung des Prüfprogramms für Rohrleitungen. Der Betreiber erstellt für seine Rohrleitungen ein Prüfprogramm, in dem er Prüfinhalt und -umfang selbst festlegt. Das Prüfprogramm muss von einer ZÜS erstmalig bestätigt und wiederkehrend auf Richtigkeit und Einhaltung überprüft werden. Die Prüfungen werden dann von einer zur Prüfung befähigten Person übernommen.

Mit der TRBS 1201 Doppelprüfungen vermeiden

Unter bestimmten Voraussetzungen bieten auch die Technische Regel TRBS 1201 und die damit verknüpfte Empfehlung EmpfBS 1201 Ansätze, um Doppelprüfungen von Arbeitsmitteln zu vermeiden und somit die Effizienz zu steigern. So fördert sie die Anerkennung der Ergebnisse von bereits vorgenommenen Prüfungen aus anderen Rechtsbereichen. Durch die Integration dieser Prüfungen in bestehende Management-Systeme und eine umfassende Dokumentation wird Transparenz geschaffen, die eine unnötige Wiederholung von Prüfungen vermeidet und die Sicherheitsstandards effektiv

unterstützt. Das trägt maßgeblich dazu bei, den bürokratischen Aufwand zu minimieren, während die Sicherheit durch zielgerichtete und sinnvolle Prüfungen gewährleistet bleibt.

Fazit

Die ÜAnIV bietet die Chance, die Sicherheit von überwachungsbedürftigen Anlagen in der Praxis effizient auszugestalten. Dabei muss das Rechtsziel eines sicheren Betriebs gewährleistet bleiben. Dafür ist

teilweise eine detaillierte Dokumentation unverzichtbar. Zugleich unterstützen Zugelassene Überwachungsstellen die Betreiber, gesetzliche Vorgaben so effektiv und effizient wie möglich umzusetzen. Das geschieht zum Beispiel mit individuellen Prüfungskonzepten und der Übernahme von vorhandenen Prüfergebnissen. Ein Wegfall der Erlaubnispflicht sollte mit planungsbegleitenden Prüfungen kompensiert werden.



KI in der Anlagensicherheit

Man muss immer das KI-Gesamtsystem denken

Künstliche Intelligenz (KI) gewinnt in der Anlagensicherheit rasch an Bedeutung. Die Echtzeitanalyse großer Datenmengen hilft dabei, potenzielle Risiken früh und effizient zu identifizieren. Gerade bei überwachungsbedürftigen Anlagen werden Beschäftigte entlastet, selbst automatisierte Reaktionen erscheinen zunehmend möglich. Doch wie steht es um Risiken und Nebenwirkungen der KI-Tools?

Herr Steimers, welche Rolle spielt KI im Bereich der Anlagensicherheit?

Eine große und überwiegend hilfreiche: KI und maschinelles Lernen können Anlagenbetreiber dabei unterstützen, komplexe Datenströme zu analysieren, Muster zu erkennen – und eben auch Musterabweichungen. Im Zuge von Industrie 4.0 liefern vernetzte Sensoren in Industrieanlagen Unmengen von Daten. Wenn man diese mit KI-Methoden analysiert, ergeben sich viele fortschrittliche Überwachungs-, Steuerungs- und Diagnosefunktionen. Die Betreiber können frühzeitig Risiken erkennen, die Effizienz verbessern und schneller auf Sicherheitsbedrohungen reagieren.

Risiken erkennen: Meinen Sie Störfälle und Attacken?

Nicht nur diese, sondern auch den Wartungsbedarf. Die Vorhersagemodelle ermöglichen Predictive Maintenance, also vorausschauende Instandhaltung. Ein informierter Anlagenbetreiber ergreift früh genug Maßnahmen, um Ausfälle zu vermeiden und so die Verfügbarkeit und Zuverlässigkeit zu steigern. Doch natürlich: Mit der zunehmenden Vernetzung und Digitalisierung industrieller Anlagen wächst auch die Bedrohung durch ausgefeilte Cyberangriffe.

Was tun Unternehmen konkret, um mit KI ihre überwachungsbedürftigen Anlagen sicherer zu machen?

KI-Algorithmen können helfen, Anomalien oder ungewöhnliche Verhaltensweisen in den Anlagen zu erkennen. IBM beispielsweise setzt in

der sogenannten Industrial Security KI-gestützte Lösungen ein, um Angriffe auf industrielle Steuerungssysteme zu bekämpfen. In der Fertigungsindustrie verwendet Siemens KI-basierte Bildverarbeitungssysteme für die visuelle Inspektion von Produktionsanlagen, um früh Defekte festzustellen. Auch BASF nutzt KI, um Betriebsprozesse in Chemieanlagen zu optimieren und die Sicherheit zu verbessern.

Wie unterstützen Dienstleister auf diesem Feld?

Der TÜV SÜD bietet etwa mit dem Asset Monitoring Artificial Intelligence Support – kurz AMAIS – eine KI-Lösung für die sensorgestützte Überwachung von Anlagenzuständen. Mit solchen Innovationen lassen sich zum Beispiel in der chemischen Industrie auch kritische Bereiche permanent prüfen, die schwer zugänglich sind. Wie verändern

sich Wandstärken durch Korrosion und Erosion? Wie entwickelt sich ein Riss? Dem Betreiber werden alle Informationen und Handlungsoptionen auf einem Dashboard angezeigt, bei Überschreiten definierter Schwellenwerte löst das System Alarm aus. Weil die KI auch Zusammenhänge erkennt, kann sie Hinweise zu einer angepassten Prozessführung liefern. Das sind schon große Vorteile.

All das macht ein Anlagenbetreiber aus eigenem Interesse. Hat ein externer Prüfer noch weitere KI-Tools in seinem Instrumentenkasten?

Wenn ein Prüfer eine Kamera an eine Drohne hängt und Bilder auswertet, kann er natürlich auch KI einsetzen, um kleine Dinge aufzuspüren, die das menschliche Auge nicht sieht. Auch autonome Roboter könnte man mit Kamerasystemen und Sensoren

herumfahren lassen. Solche kleinen KI-Helferlein könnten durchaus von Vorteil sein. Aber die Experten der Zugelassenen Überwachungsstellen, der ZÜS, laufen ja nicht nur vor Ort durch die Anlagen. Sie müssen sich auch durch einen Wust von Dokumenten arbeiten, die Anlagenbetreiber auf unterschiedlichste Art aufbereiten. Hier kann KI per Wissensmanagement und unter Einsatz von Large Language Models sehr helfen, auf die relevanten Stellen zu stoßen.

Ein ChatGPT, um Vorschriften aufzubereiten und mögliche Gefährdungen zu identifizieren?

Könnte man so nennen. Es gibt das vielversprechende Forschungsprojekt Meta-A-HAZOP des Center of Safety Excellence, CSE, das all diejenigen mit KI unterstützen will, die technische Risikoanalysen anfertigen müssen.



Bisher sitzen interdisziplinäre Teams mehrere Monate an dieser hochkomplexen Aufgabe. Im Projekt werden nun existierende HAZOP-Studien – das steht für Hazard and Operability, also Gefährdung und Betriebsfähigkeit – herangezogen, um automatisiert neue Tabellen für neue Anlagen vorzuschlagen. So will man die Risikoanalyse beschleunigen und objektivieren.

Über KI spricht man seit 50 Jahren. Woher rührt die Tempoverschärfung?

Der KI-Hype der letzten Jahre betrifft vor allem Deep Learning, also eine Unterkategorie des maschinellen Lernens, die sich mit tiefen neuronalen Netzen beschäftigt. Drei Faktoren haben die Fortschritte beschleunigt: Heute verfügt man erstens über die nötige Rechenleistung, um solche komplexe Modelle zu trainieren. Zweitens sammeln unzählige Sensoren an Produktionsanlagen genügend Daten. Und drittens teilt die Wissenschaftsgemeinschaft heute Software stärker mit anderen. Dank des kollaborativen Open-Source-Ansatzes lassen sich fertig programmierte Netze nutzen und zeitsparend auf spezifische Aufgaben weiter trainieren.

Der Durchbruch erfolgt rasant, niemand will zurückstehen – sehen Sie auch Risiken?

Der Vorteil tiefer neuronaler Netze ist zugleich ihr Nachteil: ihre unglaubliche Komplexität. Bei Hunderten Millionen Parametern haben Sie keine Chance mehr, zu verstehen, welche Verknüpfungen wirklich ablaufen. Das Problem der Erklärbarkeit, die sogenannte Explainability, bereitet massive Schwierigkeiten bei der Prüfbarkeit. Man sollte sich mitunter fragen, ob man

nicht besser auf eine andere Methode des maschinellen Lernens setzt, etwa Entscheidungsbäume, die Decision Trees. Die haben dieses Erklärbarkeitsproblem nicht.

Man sollte den Fortschritt nicht unbedingt voll ausreizen?

Genau. Mein wichtigster Grundsatz: Wenn man etwas mit einer klassischen Technologie machen kann, sollte man es damit auch machen. KI sollte man erst dann einsetzen, wenn die Aufgabe so komplex ist, dass man mit dem klassischen Verfahren nicht mehr weiterkommt. Das wird heute oft übersehen, weil eben tiefe neuronale Netze der Hype sind.

Wie funktioniert die bewährte Alternative?

Entscheidungsbäume, als altbekanntes Verfahren des maschinellen Lernens, liefern in vielen Bereichen noch immer sehr gute Ergebnisse, die vor allem für einen Menschen wunderbar nachvollziehbar sind. Etwa bei Kesselabschaltungen: Stufe für Stufe kann man definieren, was unter welchen Bedingungen zu tun ist – mit Parametern wie Druck, Temperatur oder Vibration. Das lässt sich beliebig tief gestalten – und überprüfen. Würde in diesem Baum die Schuhgröße des Prüflingenieurs als Entscheidungskriterium stehen, also totaler Unsinn, kann man es relativ einfach rausschmeißen. Bei tiefen neuronalen Netzen hat man hingegen kaum eine Chance mehr, das herauszubekommen. Höchstens über exzessive Testungen.

Was bedeutet das für die Denkweise in der Anlagensicherheit?

Wir müssen bei KI immer sehr viele Versuche durchführen, um genau die

Grenzen des Systems auszuloten. Es geht nicht darum, zu beweisen, dass es funktioniert. Sondern eher herauszubekommen, wo es gerade nicht mehr funktioniert.

Ist menschliches Vorstellungsvermögen nötig, um diese Negativfälle zu antizipieren?

Absolut. Diese Kreativität ist schon beim Zusammenstellen der Datensätze nötig. Dann aber auch auf der Prüferseite. Der Prüfer muss sich die gleichen Gedanken machen, was im Detail zu Schwierigkeiten führen kann. Bei kameragestützten Systemen ist es oft der fehlende Kontrast – was im Fall von selbstfahrenden Autos schon mehrfach tödlich endete und noch nicht im Griff ist.

Was lehrt uns das für Anlagensicherheit und den dortigen Umgang mit KI?

Es zeigt uns, dass man immer das KI-Gesamtsystem denken muss, inklusive der Hardwareprobleme, zum Beispiel bei Kameras. Im KI-Bereich hat man überwiegend mit programmieraffinen Informatikern zu tun. Die denken nicht unbedingt so weit, dass die Hardware ein Problem haben könnte. Doch falls das so ist, kann unser KI-Modell so gut sein, wie es will...

Ganz simpel gefragt: Kann man Künstlicher Intelligenz vertrauen?

Die lange Antwort hätte Schnittmengen zur Philosophie. Die EU-Kommission identifiziert jedenfalls drei wesentliche Elemente für eine vertrauenswürdige KI: Sie muss rechtmäßig sein, ethisch und robust. Gerade beim Punkt Ethik sollten wir uns verstärkt Gedanken machen über Kontrollfragen: Wie automatisiert

soll ein System überhaupt sein? Bei bestimmten Anwendungen will man einfach, dass der Mensch eingreifen kann oder Entscheidungen am Ende freigegeben muss.

Zum Beispiel?

Nehmen Sie Personalentscheidungen, bei denen Diskriminierungsfreiheit geboten ist. Vielleicht ist es da schön, wenn eine assistierende KI mal Empfehlungen ausspricht. Aber im Grunde braucht es keinen hohen Automatisierungsgrad und viele Beispiele belegen die Gefahr: Denn wenn die historischen Trainingsdaten auf Vorurteilen beruhen, wird Diskriminierung reproduziert.

Bei der Anlagensicherheit geht es ja nicht um Recruiting, sondern um Druckkessel und Aufzüge.

Dürfen wir dort KI etwas sorgloser einsetzen?

So einfach ist es nicht. Auch bei Anlagensicherheit kann Diskriminierungsfreiheit schnell relevant werden – etwa beim Einsatz von Kamerasystemen in Schutzzonen, die niemand

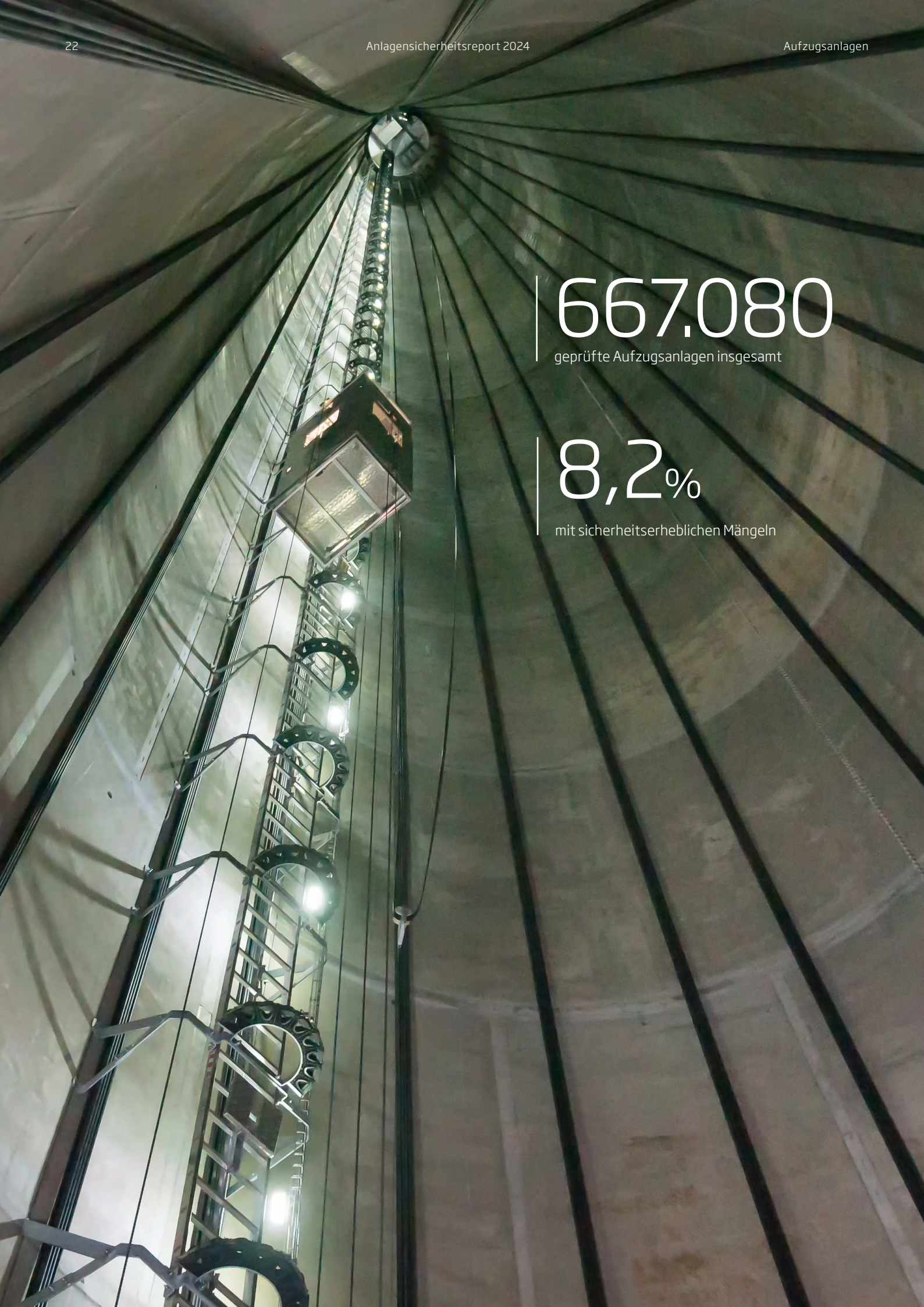
betreten soll. Das berührt neben Fairness-Fragen zugleich die Zuverlässigkeit, wenn Trainingsdaten vor allem auf weißen Männern beruhen. Reden wir über die Maschinenüberwachung mit Sensoren, ist das tatsächlich weniger relevant.

Also ist es vor allem ein Problem der Arbeitssicherheit?

Ja. Ein konkretes Beispiel betrifft einen Hersteller von Formatkreissägen für Schreinereibetriebe. Bei dieser Arbeit muss man ein Werkstück durch das Sägeblatt schieben – Lichtschranken bringen zum Schutz wenig. Ein Hersteller hatte die Idee, mit Deep-Learning-Modellen Hände zu erkennen und ihre Bewegungspfade vorherzusagen. Ein Ausrutschen würde blitzschnell das Sägeblatt stillsetzen. Das KI-gestützte Assistenzsystem erhöht die Sicherheit. Aber auch hier: Was ist mit tätowierten Händen? Oder solchen, die schon nicht mehr über fünf Finger verfügen? Es besteht bei KI immer die Gefahr, dass sie die seltenen Fälle übersieht.



André Steimers ist Professor an der Hochschule Koblenz und dort Experte für vertrauenswürdige Künstliche Intelligenz. Nach Stationen beim TÜV NORD und beim Institut für Arbeitsschutz wirkt er in zahlreichen Gremien zur KI-Normung mit und beleuchtet Risikoanalyse-Methoden in diesem Bereich.

A low-angle, upward-looking photograph of an elevator shaft. The concrete walls of the shaft are visible, with numerous steel cables fanning out from the top. An elevator car is visible in the middle of the shaft, and several counterweights are positioned along the shaft's length. The lighting is dim, with some light coming from the car and the counterweights.

667.080

geprüfte Aufzugsanlagen insgesamt

8,2%

mit sicherheitserheblichen Mängeln

Prüfungen von Aufzugsanlagen

Die Sicherheit von Aufzugsanlagen wird in Deutschland engmaschig überwacht. Im jährlichen Wechsel findet eine umfangreiche Hauptprüfung und eine Zwischenprüfung statt. Hinzu kommen Prüfungen nach prüfpflichtigen Änderungen, zum Beispiel nach dem Austausch besonders sicherheitskritischer Bauteile und Prüfungen nach Wiederinbetriebnahme. Gesondert ausgewiesen werden die ebenfalls obligatorischen Prüfungen vor der erstmaligen Inbetriebnahme.

Im Jahr 2023 haben die Sachverständigen der Zugelassenen Überwachungsstellen (ZÜS) 667.080 Aufzugsanlagen geprüft. Mit einem Anteil von 48,9 Prozent war nach Abschluss der Prüfung nur knapp die Hälfte der Aufzüge mängelfrei. 42,6 Prozent der untersuchten Aufzüge wiesen geringfügige Mängel auf und 8,2 Prozent sicherheitserhebliche Mängel. Bei 0,3 Prozent der Aufzugsanlagen stellten die Sachverständigen gefährliche Mängel fest. Das entspricht rund 2.000 Anlagen.

Die Bewertung der Mängel erfolgt auf Grundlage eines Beschlusses des Erfahrungsaustauschkreises der Zugelassenen Überwachungsstellen (EK ZÜS).¹ Im entsprechenden Mängelkatalog sind drei Mängelkategorien für Aufzüge festgelegt:

- > **Geringfügige Mängel müssen bis zur nächsten wiederkehrenden Prüfung behoben werden.**
- > **Sicherheitserhebliche Mängel müssen spätestens nach drei Monaten behoben sein. Nach der Behebung erfolgt eine Nachprüfung durch die ZÜS.**
- > **Gefährliche Mängel gefährden Benutzer:innen sowie Wartungs- und Prüfpersonal unmittelbar. Aufzüge mit gefährlichen Mängeln werden sofort stillgelegt.**

Prüfungen vor Inbetriebnahme

Seit dem Jahr 2017 prüfen die Sachverständigen der ZÜS neue Aufzugsanlagen auch vor der erstmaligen

Inbetriebnahme (PvI). Prüfgrundlagen sind die Aufzugsrichtlinie 2014/33/EU (AufzRL) oder die Maschinenrichtlinie 2006/42/EG (MaschRL). Unter die MaschRL fallen neben Homelifts auch bestimmte barrierefreie Aufzugsanlagen für Menschen mit Behinderungen und Fassadenbefahranlagen sowie Aufzüge in den Türmen von Windenergieanlagen. Zu den Aufzügen nach AufzRL gehören Personen- und Lastenaufzüge, die ein Betreten von Personen zulassen und nicht unter die MaschRL fallen.

Im Jahr 2023 haben ZÜS-Sachverständige insgesamt 27.262 Aufzüge vor erstmaliger Inbetriebnahme geprüft. 20,4 Prozent der Anlagen hatten geringfügige Mängel, 10,4 Prozent sicherheitserhebliche Mängel und 4,2 Prozent gefährliche Mängel.

1) Aktueller Beschluss ZÜS-BA-002 rev 7.

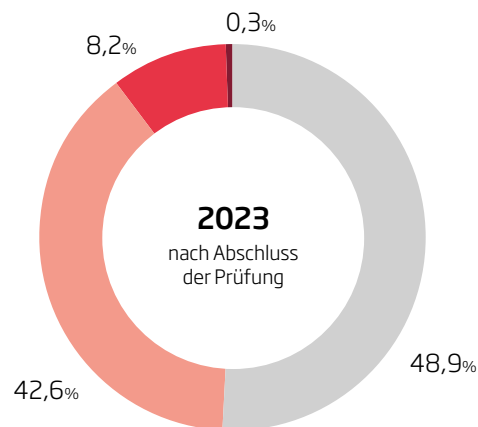
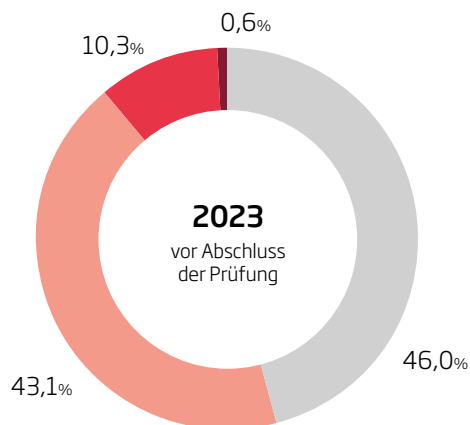
Aufzugsanlagen

Alle Mängel bei wiederkehrenden Prüfungen: Haupt- und Zwischenprüfung

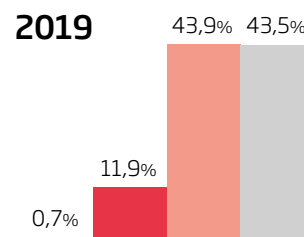
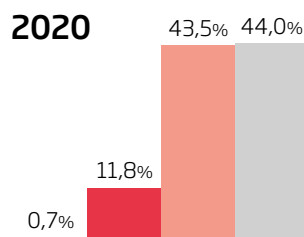
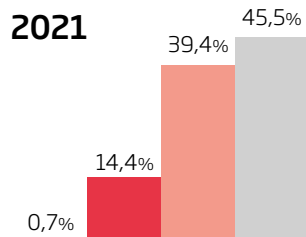
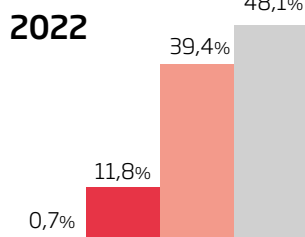
667.080

Gesamtzahl der wiederkehrenden Prüfungen

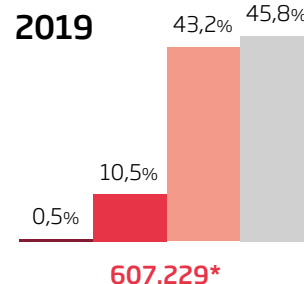
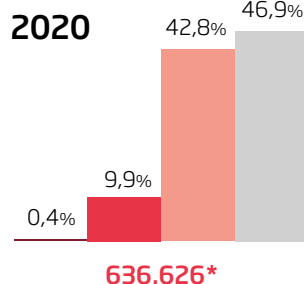
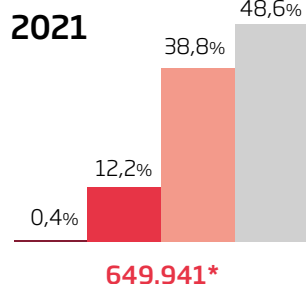
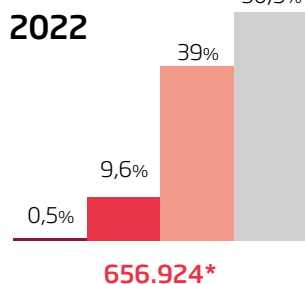
- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



vor Abschluss der Prüfung



nach Abschluss der Prüfung



* Gesamtzahl der Prüfungen

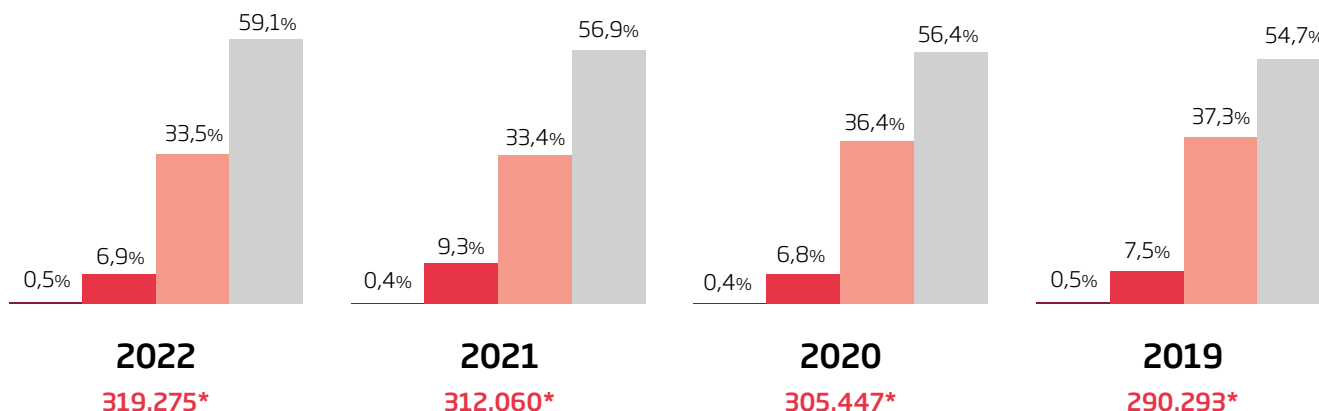
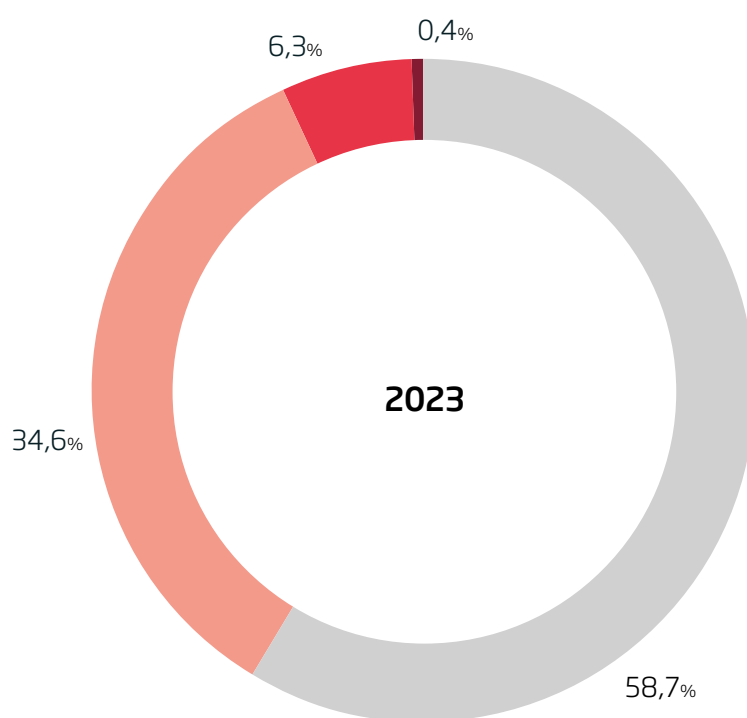
Aufzugsanlagen

Bei Zwischenprüfungen festgestellte Mängel

324.136

Gesamtzahl der Zwischenprüfungen

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



* Gesamtzahl der Prüfungen

Zwischenprüfungen finden unangekündigt im jährlichen Wechsel mit der angekündigten Hauptprüfung statt

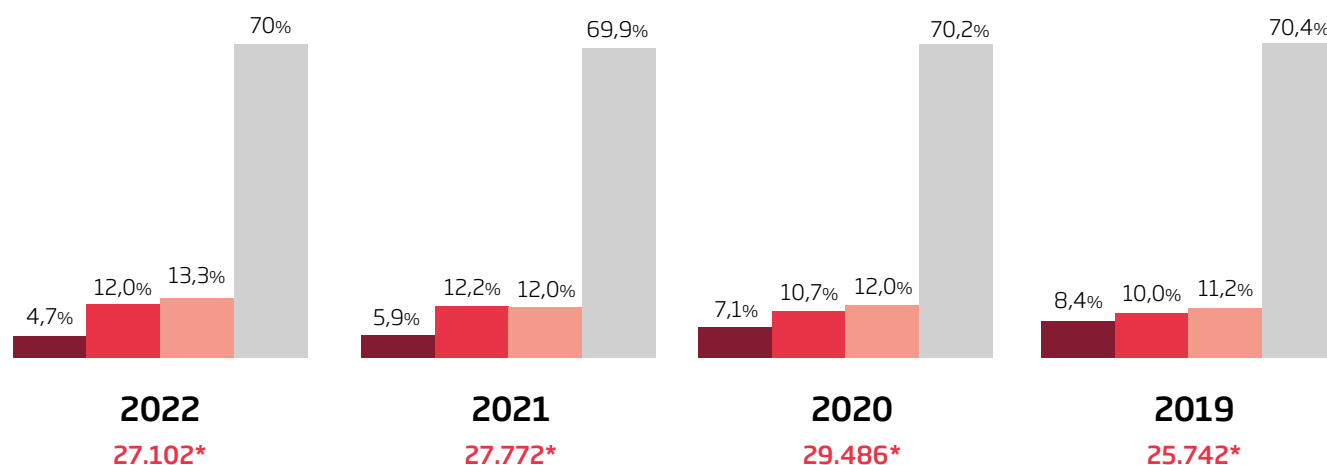
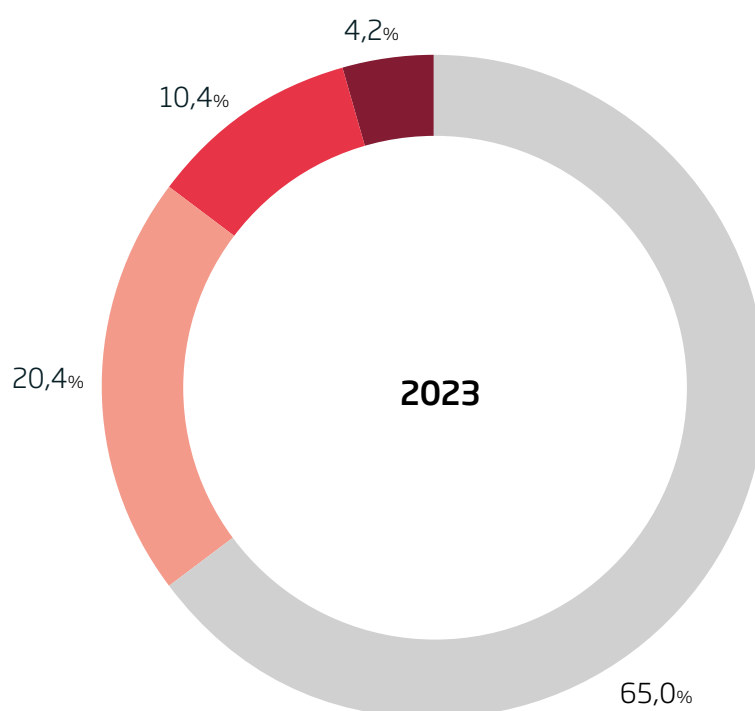
Aufzugsanlagen

Bei Prüfungen vor erstmaliger Inbetriebnahme festgestellte Mängel

27.262

Gesamtzahl der Prüfungen vor erstmaliger Inbetriebnahme nach 2014/33/EU und 2006/42/EG

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



* Gesamtzahl der Prüfungen

Aufzugsanlagen

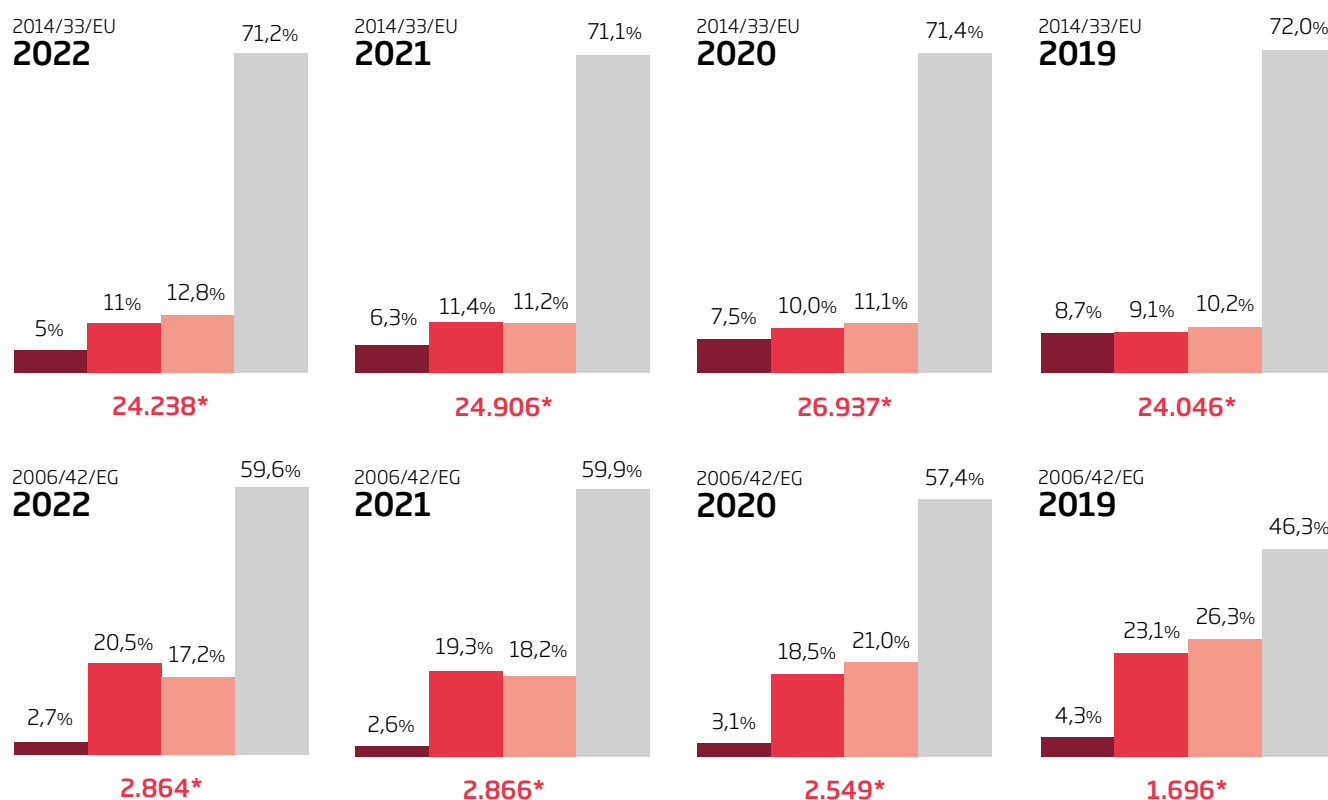
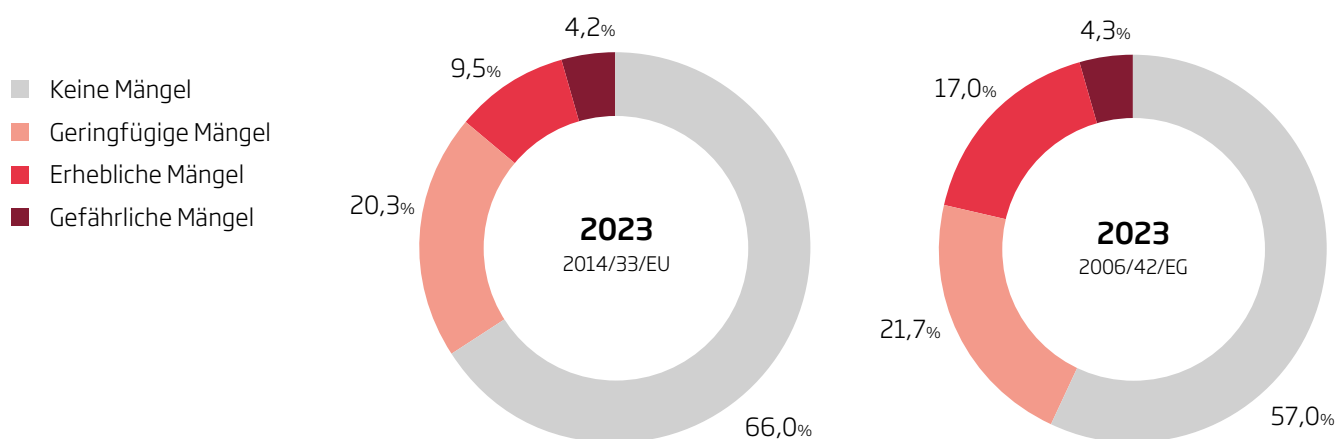
Bei Prüfungen vor erstmaliger Inbetriebnahme festgestellte Mängel

24.286

Prüfungen nach
2014/33/EU

2.976

Prüfungen nach
2006/42/EG



* Gesamtzahl der Prüfungen

| 291.877

geprüfte Druckbehälteranlagen

| 5,0%

mit erheblichen Mängeln

| 80,9%

ohne Mängel



Prüfungen von Druckanlagen

Druckbehälteranlagen sind Anlagen mit einem Volumen von mindestens einem Liter und einem maximal zulässigen Druck von mehr als 0,5 bar. Zu ihnen zählen beispielsweise Druckluftbehälter bei Kompressoren oder Reaktionsbehälter in verfahrenstechnischen Anlagen.

Im Jahr 2023 prüften die Sachverständigen der Zugelassenen Überwachungsstellen (ZÜS) insgesamt 291.877 Druckanlagen. Davon waren 80,9 Prozent mängelfrei, 14,0 Prozent wiesen geringfügige Mängel auf und 5,0 Prozent erhebliche Mängel. 0,1 Prozent der Anlagen wiesen gefährliche Mängel auf. Rund 290 Anlagen fielen in diese Mängelkategorie. Die Betreiber müssen diese Anlagen unverzüglich außer Betrieb nehmen.

Dampfkesselanlagen beinhalten beheizte Druckgeräte, bei denen die

Gefahr einer Überhitzung besteht. Sie erzeugen Dampf oder Heißwasser mit einer Temperatur von mehr als 110 Grad bei einem Volumen von mehr als 2 Litern und einem maximal zulässigen Druck von mehr als 0,5 bar. Zu dieser Anlagenkategorie gehören Kraftwerkskessel oder auch Dampferzeuger für Sterilisatoren in Krankenhäusern. Bei den 26.625 im Jahr 2023 geprüften Dampfkesselanlagen wurden bei 77,4 Prozent der Anlagen keine Mängel festgestellt. 18,1 Prozent wiesen geringfügige und 4,4 Prozent erhebliche Mängel auf. Gefährliche Mängel wurden bei 0,1 Prozent der Anlagen festgestellt.

Die Bewertung der Mängel erfolgt auf Grundlage eines Beschlusses des Erfahrungsaustauschkreises der Zugelassenen Überwachungsstellen vom 15. November 2017 in der zum Prüfungszeitpunkt gültigen Fassung.¹ Darin wurden drei spezifische Mängel-

kategorien für Druckanlagen festgelegt:

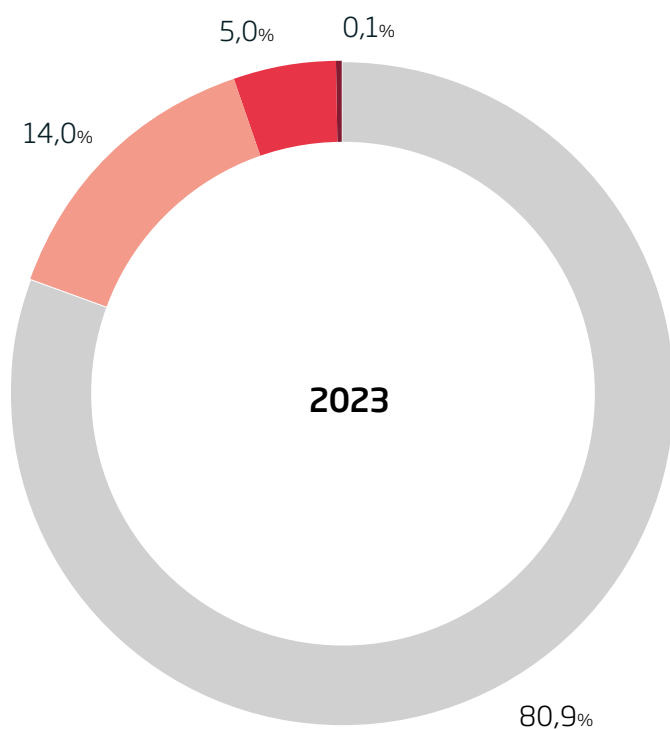
- > geringfügig
- > erheblich
- > gefährlich

Die Zuordnung zu diesen Kategorien erfolgt auf Basis einer zusammenfassenden Bewertung der aufgetretenen Einzelmängel. Ein erheblicher Mangel kann also durchaus auch mehrere erhebliche oder geringfügige Einzelmängel beinhalten. Diese Beschränkung auf die Erfassung und Darstellung des Prüfergebnisses ist erforderlich, um grundlegende Aussagen über den sicherheitstechnischen Standard der Anlagen zu erhalten und einen bundesweit einheitlichen Überblick unter Einbeziehung aller ZÜS zu erreichen.

1) Aktueller Beschluss ZÜS-BD-003 rev 7.

Druckbehälteranlagen

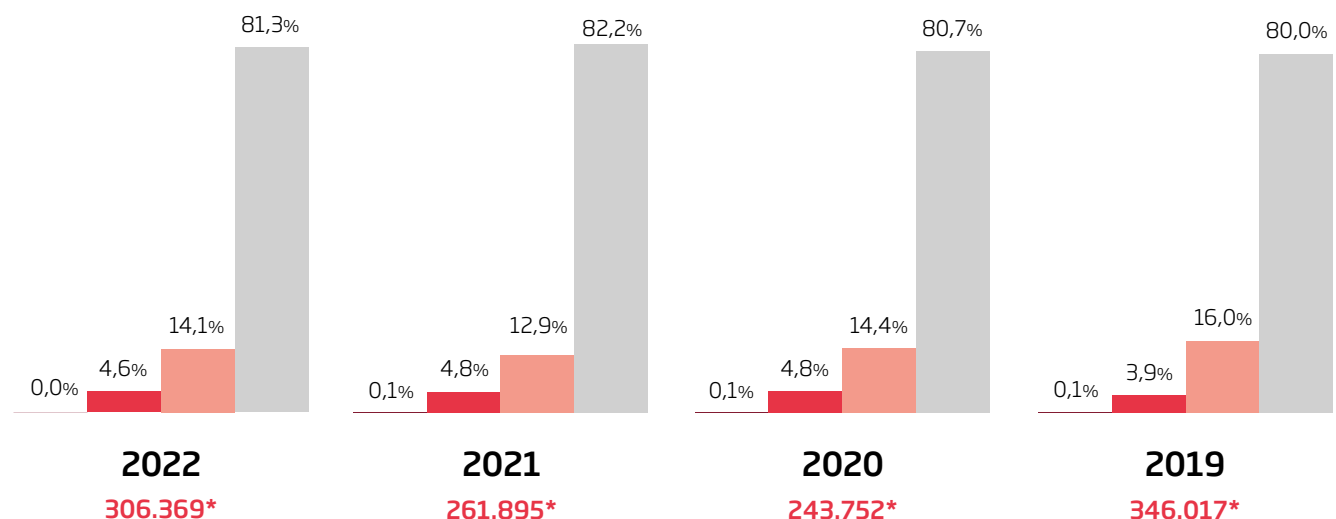
Mängelverteilung über alle Prüfungen von Anlagen und Anlagenteilen



291.877

Gesamtzahl der Prüfungen von Anlagen und Anlagenteilen

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



* Gesamtzahl der Prüfungen

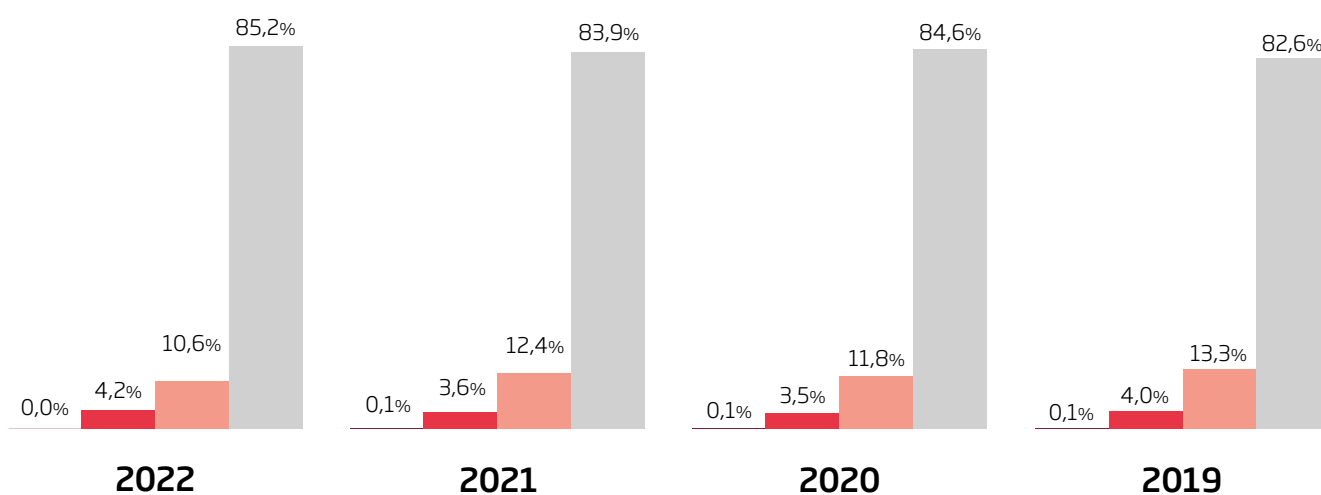
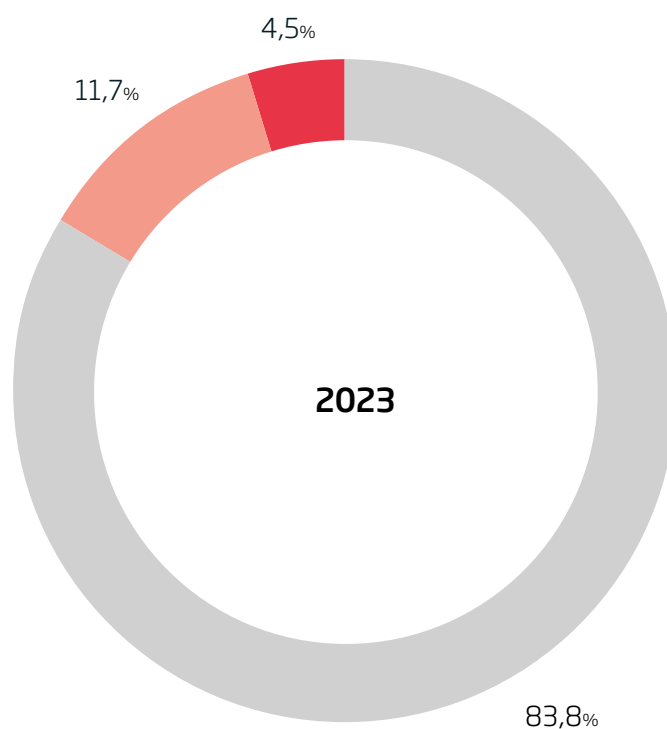
Druckbehälteranlagen

Festgestellte Mängel bei Prüfung vor Inbetriebnahme

83,8%

aller geprüften Druckbehälteranlagen
bei Prüfung vor Inbetriebnahme
sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



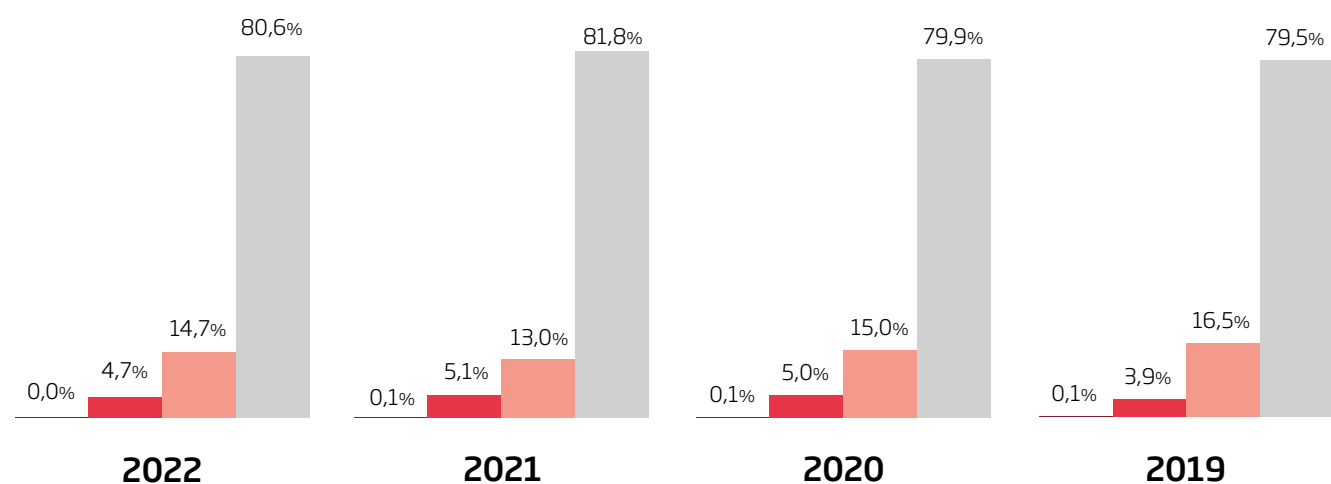
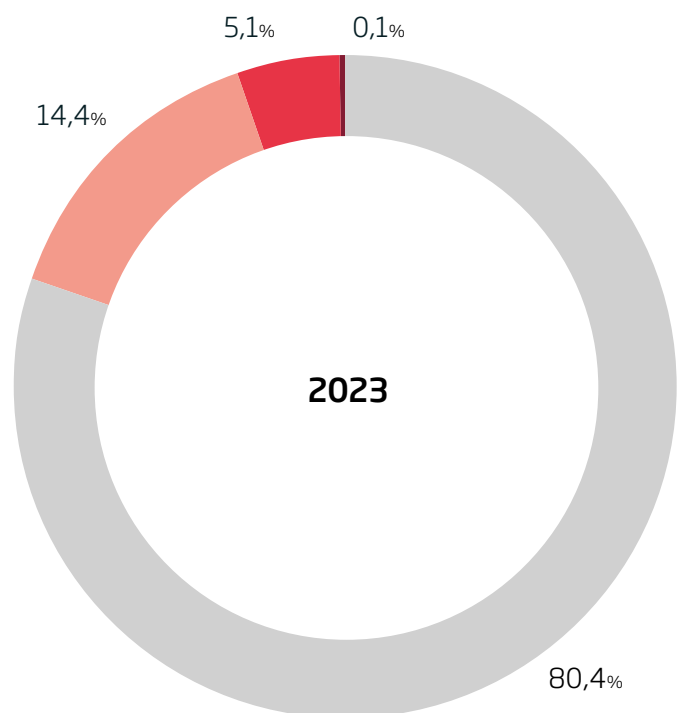
Druckbehälteranlagen

Festgestellte Mängel bei wiederkehrenden Prüfungen

80,4%

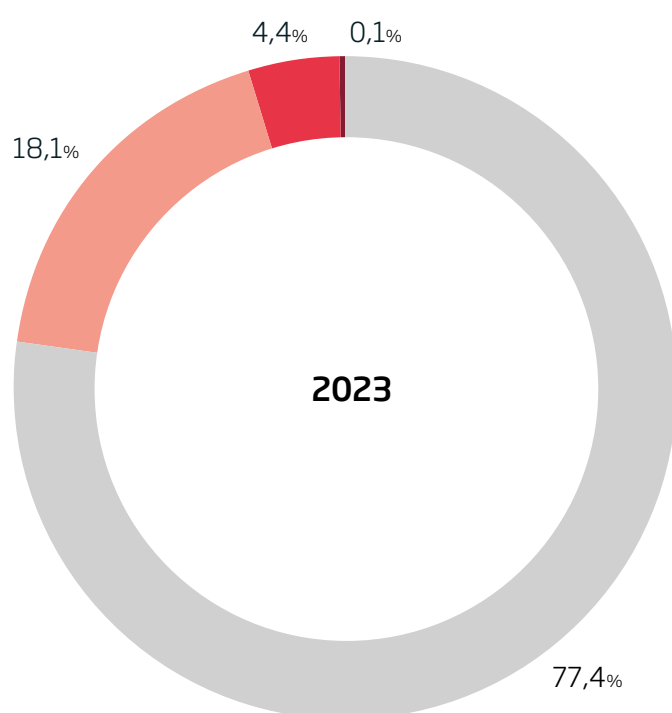
aller geprüften Druckbehälteranlagen
bei wiederkehrenden Prüfungen sind
mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



Dampfkesselanlagen

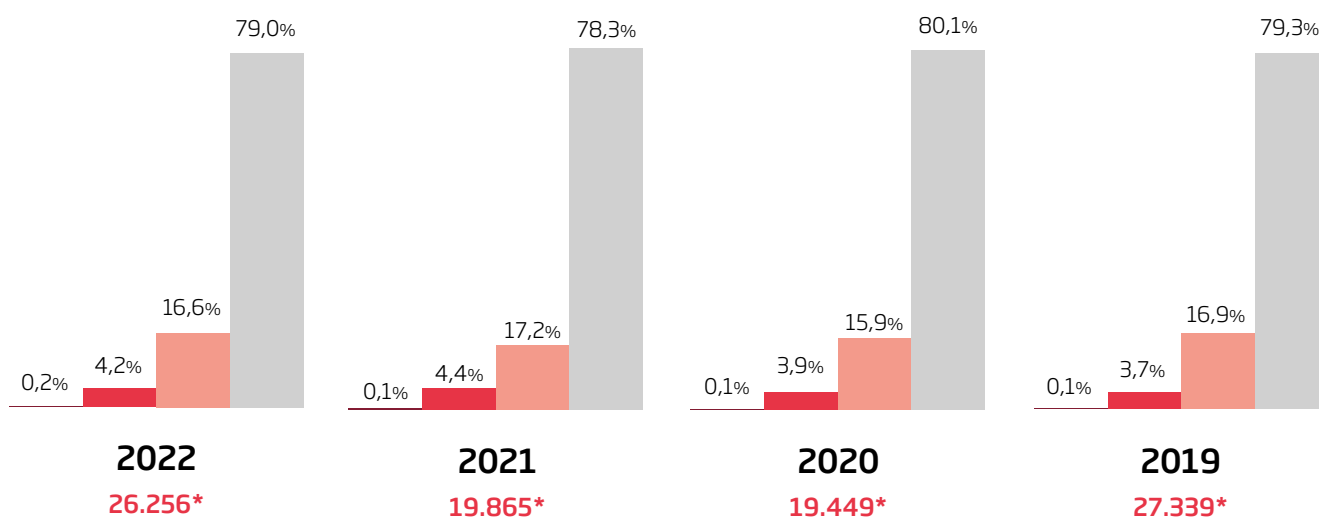
Mängelverteilung über alle Prüfungen von Anlagen und Anlagenteilen



26.625

Gesamtzahl der Prüfungen von Anlagen und Anlagenteilen

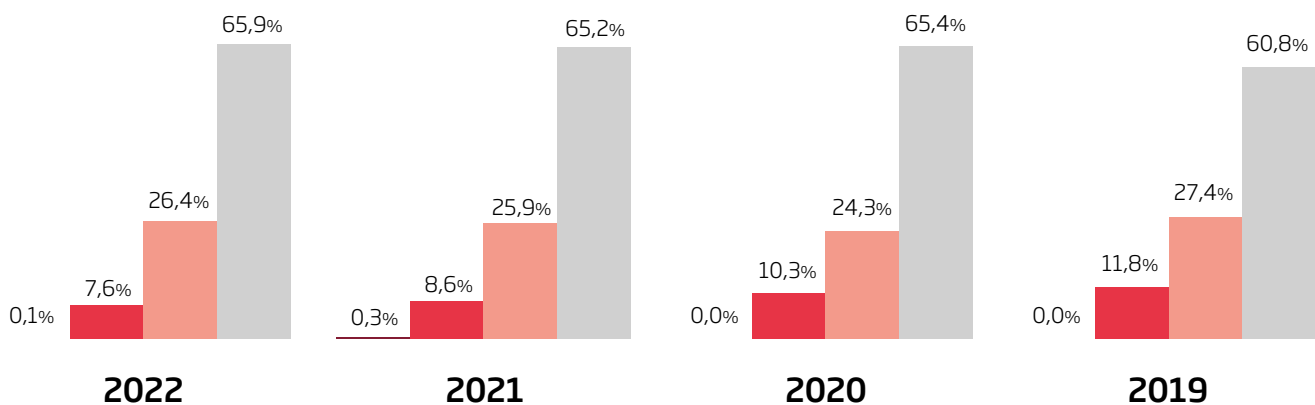
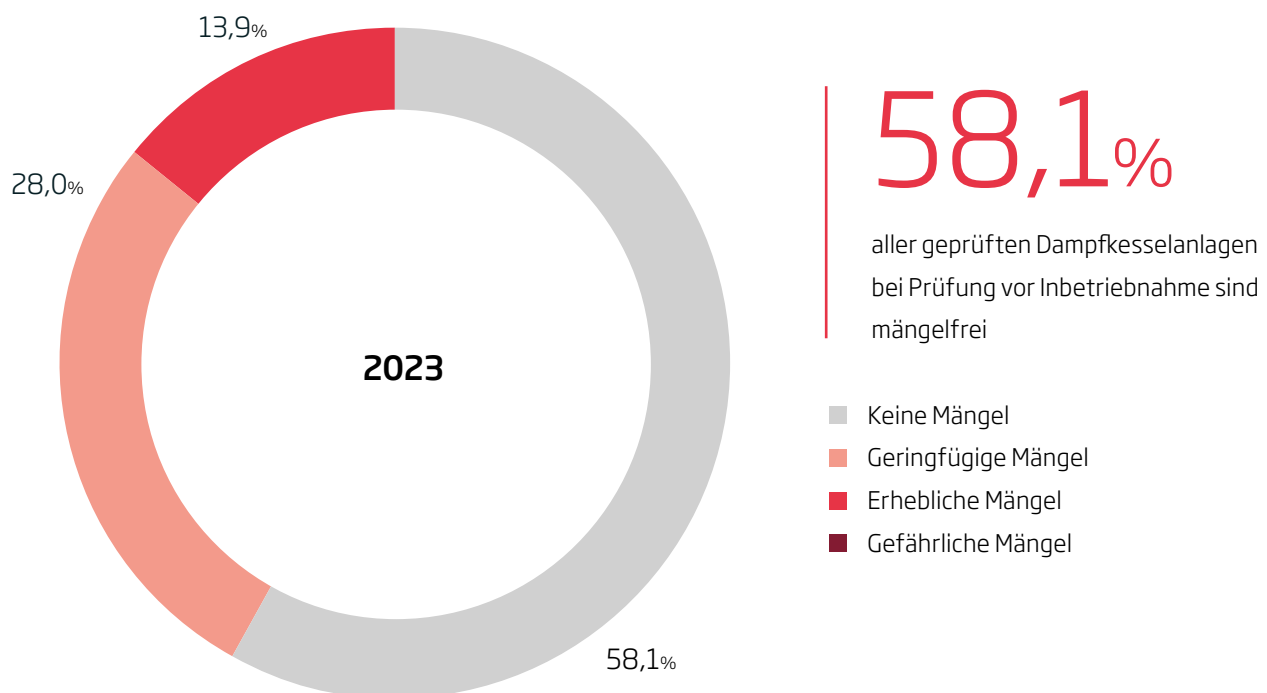
- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



* Gesamtzahl der Prüfungen

Dampfkesselanlagen

Festgestellte Mängel bei Prüfung vor Inbetriebnahme



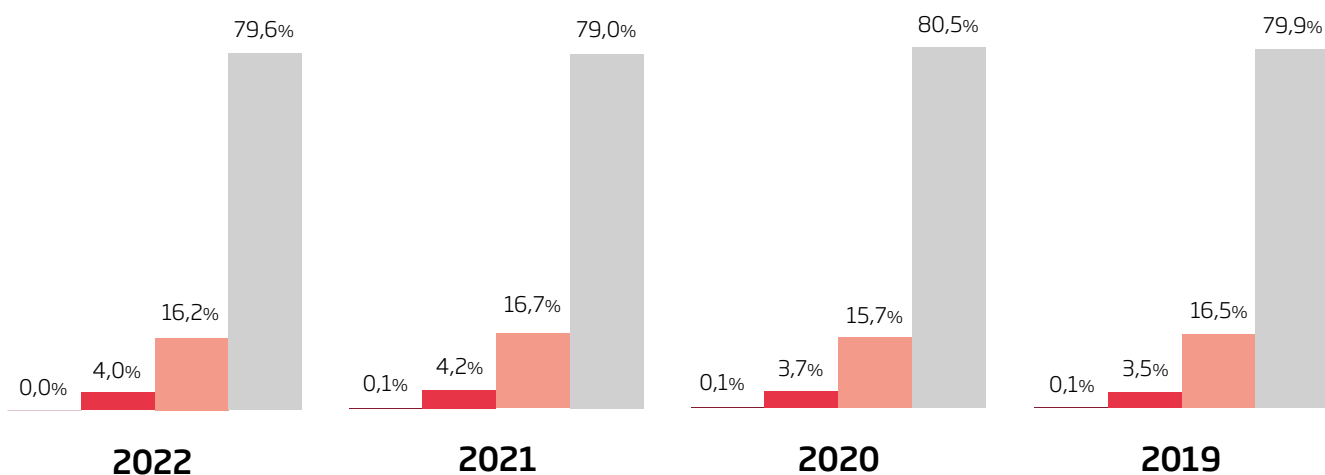
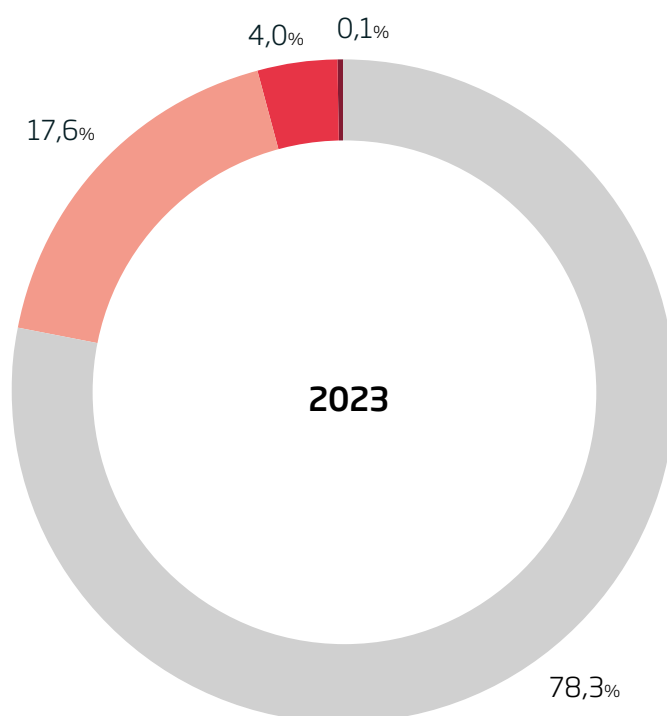
Dampfkesselanlagen

Festgestellte Mängel bei wiederkehrenden Prüfungen

78,3%

aller geprüften Dampfkesselanlagen
bei wiederkehrenden Prüfungen sind
mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



Prüfungen von Ex-Anlagen

In der Betriebssicherheitsverordnung¹ werden Ex-Anlagen als „Gesamtheit der explosionsschutzrelevanten Arbeitsmittel einschließlich der Verbindungselemente sowie der explosionsschutzrelevanten Gebäudeteile“ definiert. Dabei handelt es sich im Wesentlichen um Anlagen für

die Lagerung sowie die Befüllung und Entnahme von entzündbaren Stoffen, aber auch um verfahrenstechnische Anlagen oder Lackierkabinen. Explosionsschutzrelevante Arbeitsmittel sind beispielsweise Elektromotoren, Heizoberflächen oder Gasbrenner, die eine Zündquelle darstellen. Unter den

Gebäudeteilen versteht man unter anderem Fußböden mit erforderlicher elektrostatischer Ableitfähigkeit oder Wände, die der Abdichtung eines Raumes mit einer explosionsfähigen Atmosphäre dienen.

15.324

Summe aller geprüften Ex-Anlagen
und ihrer Anlagenteile 2023



Der Anlagensicherheitsreport führt die Mängelzahlen für folgende Ex-Anlagen auf:

- > Lageranlagen mit ortsfesten Behältern mit einem Gesamtrauminhalt von mehr als 10.000 Litern,
- > Füll- und Entleerstellen mit einer Umschlagkapazität von mehr als 1.000 Litern pro Stunde sowie
- > Tankstellen für Fahrzeuge aller Art und Flugfeldbetankungsanlagen, soweit entzündbare Flüssigkeiten nach Anhang 1 Nummer 2.6 der Verordnung (EG) Nr. 1272/2008 mit einem Flammpunkt von weniger als 23 Grad Celsius gelagert oder abgefüllt werden.

Die Zugelassenen Überwachungsstellen (ZÜS) haben für Ex-Anlagen folgende Mängelkategorien festgelegt:²

- > geringfügig
- > erheblich
- > gefährlich

Die Zuordnung zu diesen Kategorien erfolgt auf Basis einer Zusammenfassung der erfassten Einzelmängel. Eine der Mängelkategorie „erheblicher Mangel“ zugeordnete Anlage kann durchaus mehrere erhebliche oder geringfügige Einzelmängel beinhalten. Dieser Fokus auf das Prüfungsergebnis und nicht auf einzelne Mängel ermöglicht, die Ergebnisse bundesweit zu vergleichen und grundlegende Aussagen über den Sicherheitszustand der Anlagen auf Basis aller Ergebnisse der ZÜS zu treffen.

Prüfung vor Inbetriebnahme und während der Prüfung behobene Mängel

Seit dem Jahr 2011 wird zwischen Mängeln differenziert, die bei einer Prüfung vor Inbetriebnahme (PvI) erfasst werden und solchen Mängeln, die bei einer wiederkehrenden Prüfung im laufenden Betrieb entdeckt werden. Daraus lassen sich Schlüsse für die Sicherheit der Anlagen und den Prüfbetrieb ziehen.

Neben der Erfassung der Prüfergebnisse ist auch die Zahl der während der Prüfung beseitigten Mängel für die Bewertung des Anlagenzustands interessant. Dabei handelt es sich um die Mängel, die noch während der Prüfung beispielsweise durch den Austausch von sicherheitstechnischen Ausrüstungsteilen behoben werden. Bei diesen Mängeln handelt es sich um Einzelmängel, bei denen auf eine Kategorisierung verzichtet wurde.

Zustand der Ex-Anlagen im Jahr 2023

Im Jahr 2023 haben die Sachverständigen der ZÜS insgesamt 15.324 Ex-Anlagen und deren Anlagenteile vor Inbetriebnahme und wiederkehrend geprüft: Geprüft wurden 4.917 Tankstellen, 2019 Gasfüllanlagen, 978 Lageranlagen, 222 Füll- und Entleerstellen sowie 7.188 sonstige Ex-Anlagen.

Mit einem Anteil von 46,8 Prozent der geprüften Tankstellen war weniger als die Hälfte der geprüften Anlagen mängelfrei. Mehr als jede dritte Anlage

(33,8 Prozent) hatte geringfügige Mängel. 19,3 Prozent der geprüften Tankstellen wiesen erhebliche Mängel auf und 0,1 Prozent sogar gefährliche Mängel.

Bei den Gasfüllanlagen waren 43,6 Prozent der geprüften Anlagen ohne Mängel. Mehr als ein Drittel dieser Anlagen (36,2 Prozent) wurde von den Sachverständigen der Mängelkategorie „geringfügig“ zugeordnet. 19,9 Prozent der Gasfüllanlagen wurden in die Kategorie der „erheblichen Mängel“ eingestuft und ganze 0,3 Prozent gelten als gefährlich.

Von den 978 im Jahr 2023 geprüften Lageranlagen wurden bei 37,7 % keine Mängel festgestellt. Ein gutes Drittel (35,4 Prozent) hatte „geringfügige Mängel“ und 26,4 Prozent fielen in die Kategorie der Anlagen mit erheblichen Mängeln. Gefährliche Mängel wurden sogar bei 0,5 Prozent festgestellt.

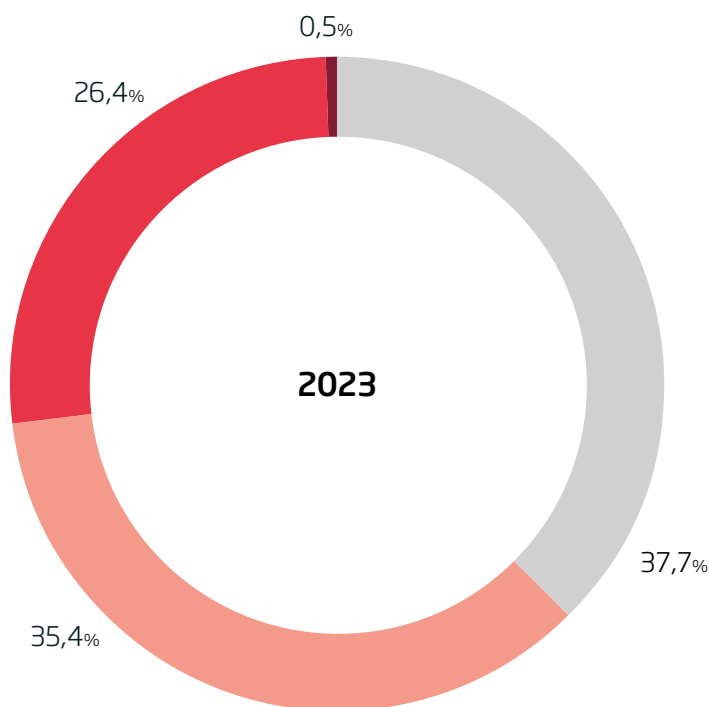
Bei 51,4 Prozent der geprüften Füll- und Entleerstellen wurden keine Mängel festgestellt. Geringfügige Mängel wurden bei 32,4 % der Anlagen festgestellt und 15,8 % fallen in die Mängelkategorie „erheblicher Mangel“.

1) Fassung vom 27. Juli 2021.

2) Aktueller Beschluss ZÜS-BE-004 rev 4.

Lageranlagen

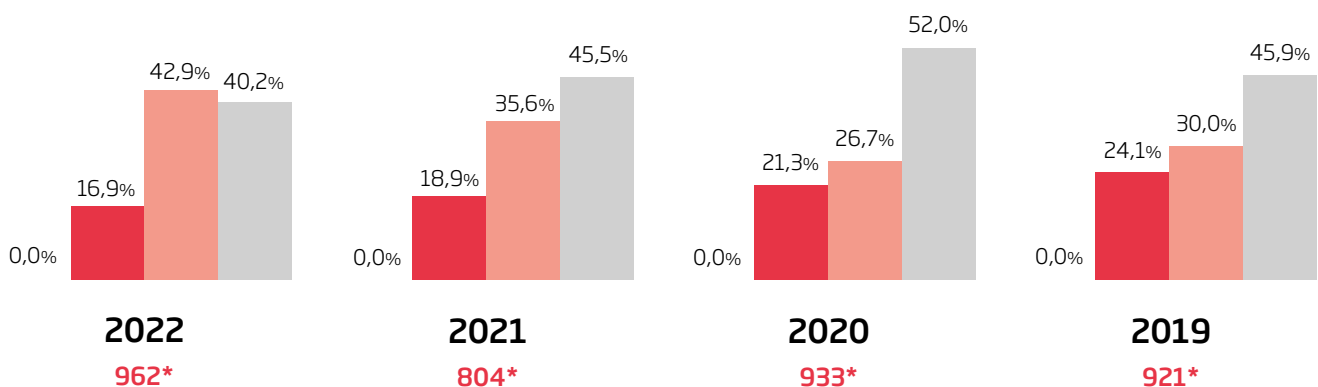
Mängelverteilung über alle Prüfungen hinweg



978

Gesamtzahl der Prüfungen von
Lageranlagen

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



* Gesamtzahl der Prüfungen

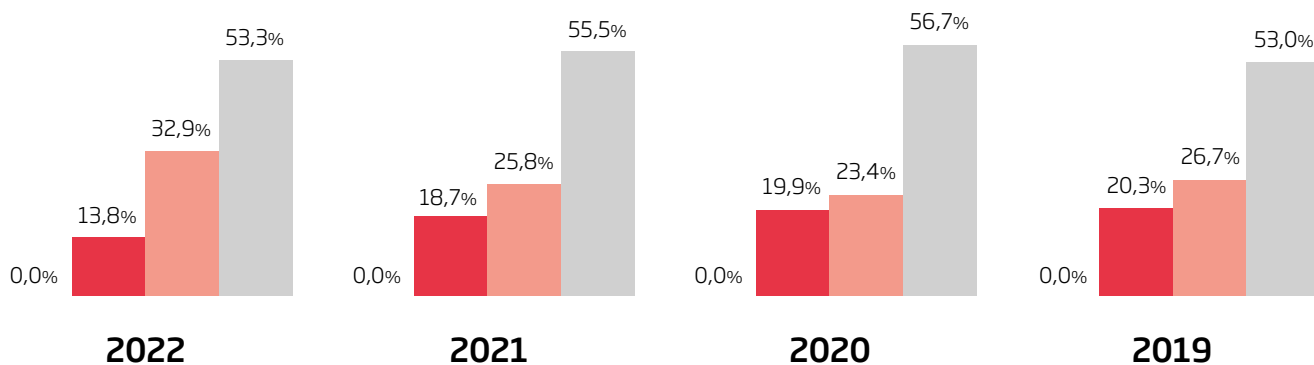
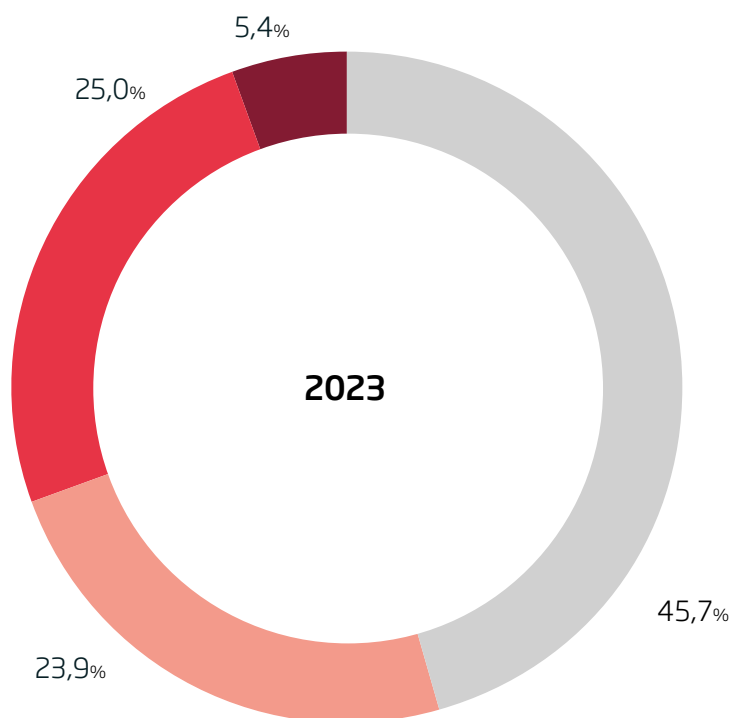
Lageranlagen

Festgestellte Mängel bei Prüfung vor Inbetriebnahme

45,7%

aller vor Inbetriebnahme geprüften
Lageranlagen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



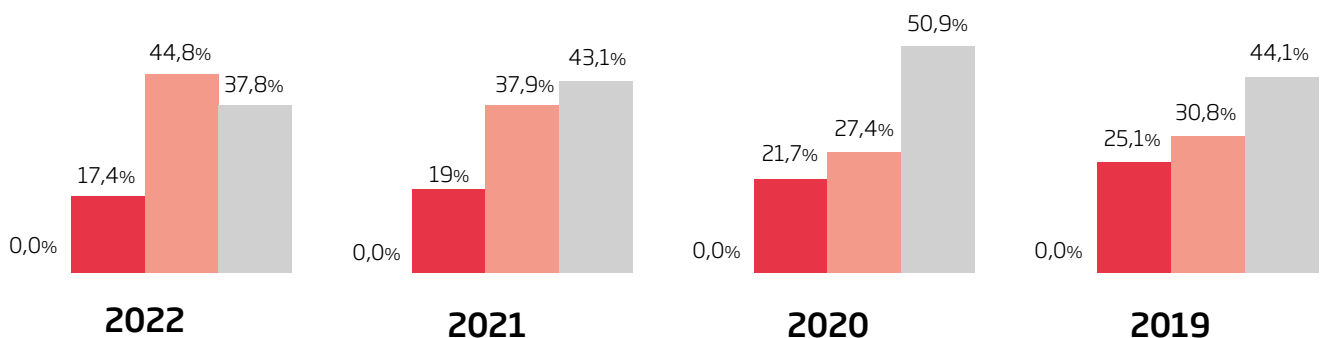
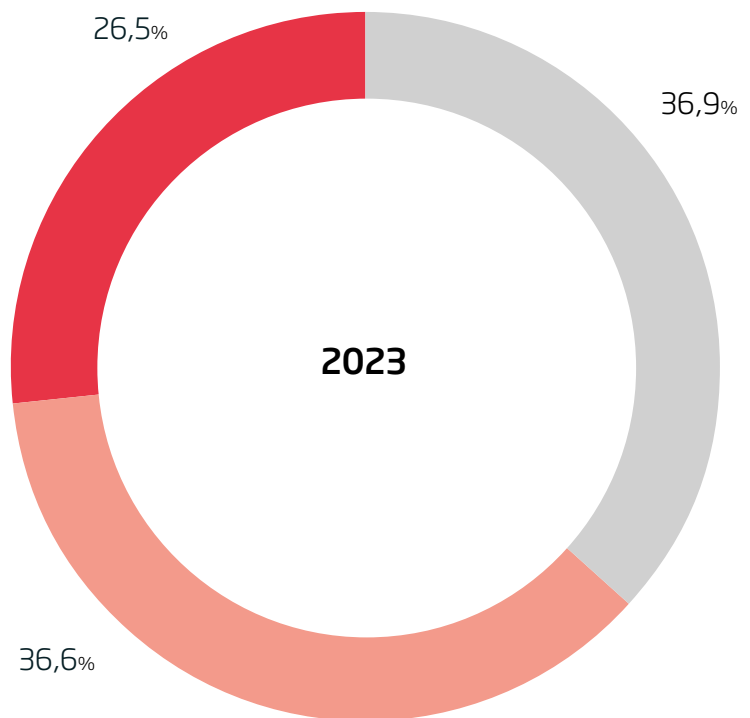
Lageranlagen

Festgestellte Mängel bei wiederkehrenden Prüfungen

36,9%

aller aller Lageranlagen bei wiederkehrenden Prüfungen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



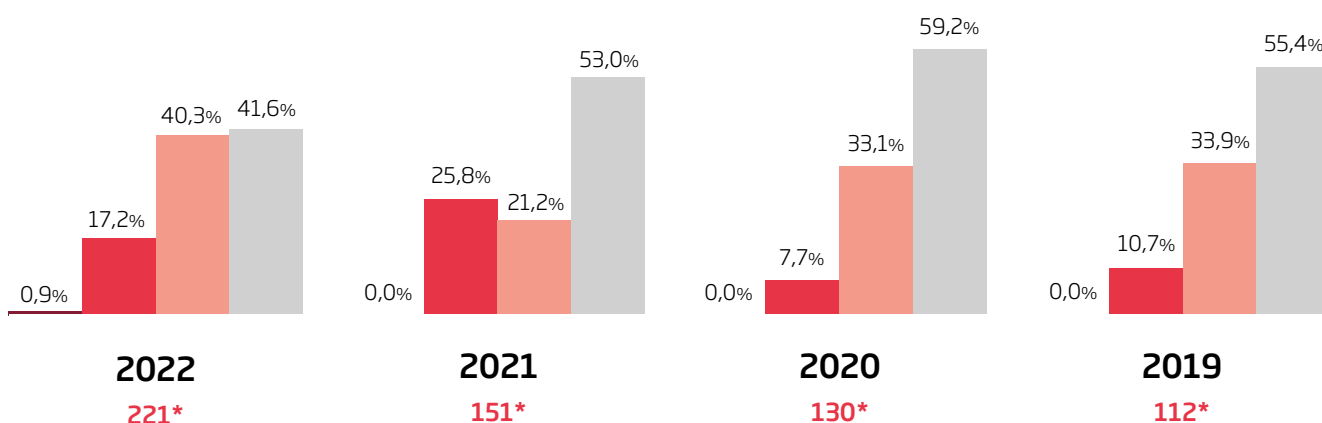
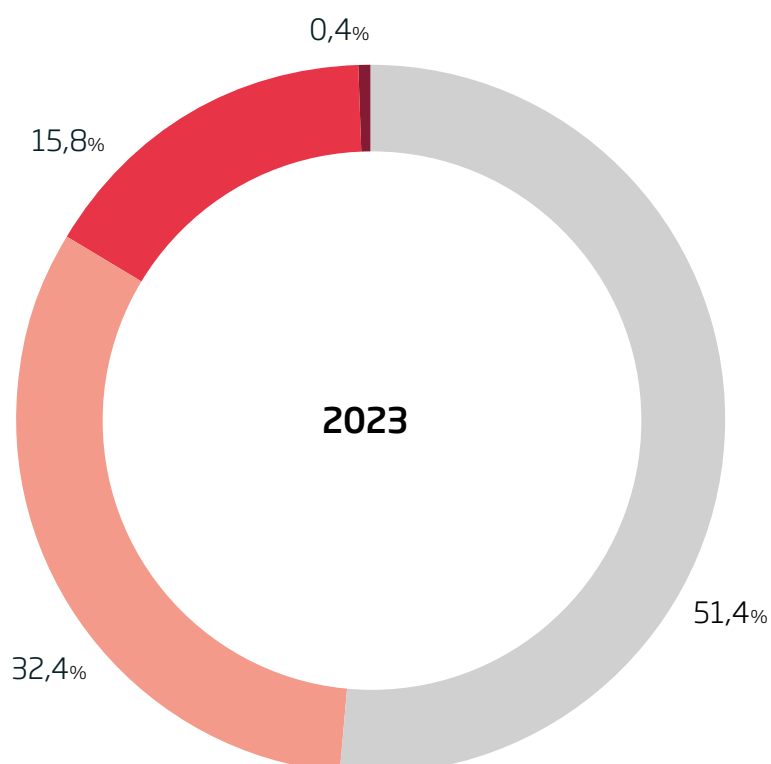
Füll- und Entleerstellen

Mängelverteilung über alle Prüfungen hinweg

222

Gesamtzahl der Prüfungen

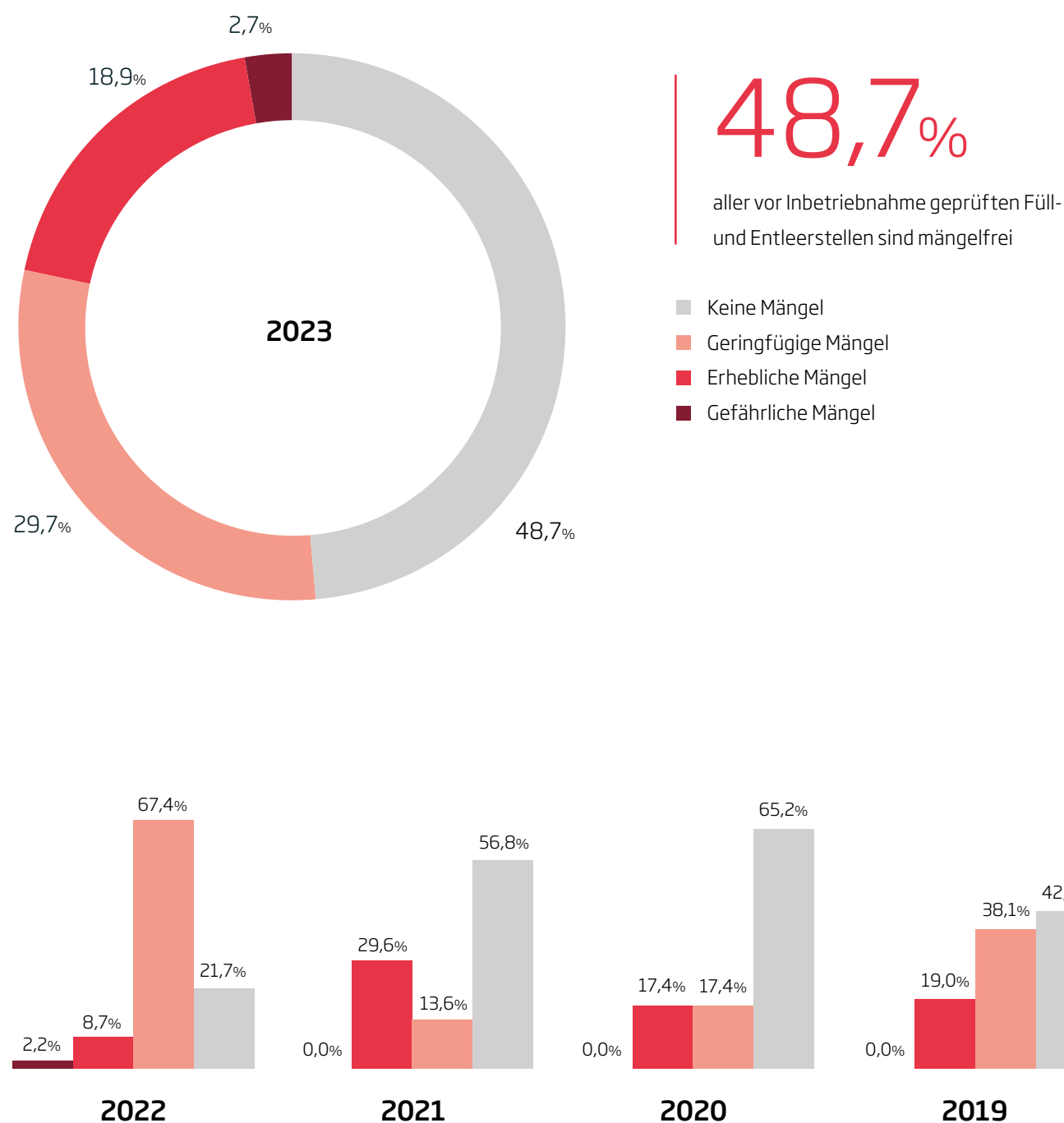
- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



* Gesamtzahl der Prüfungen

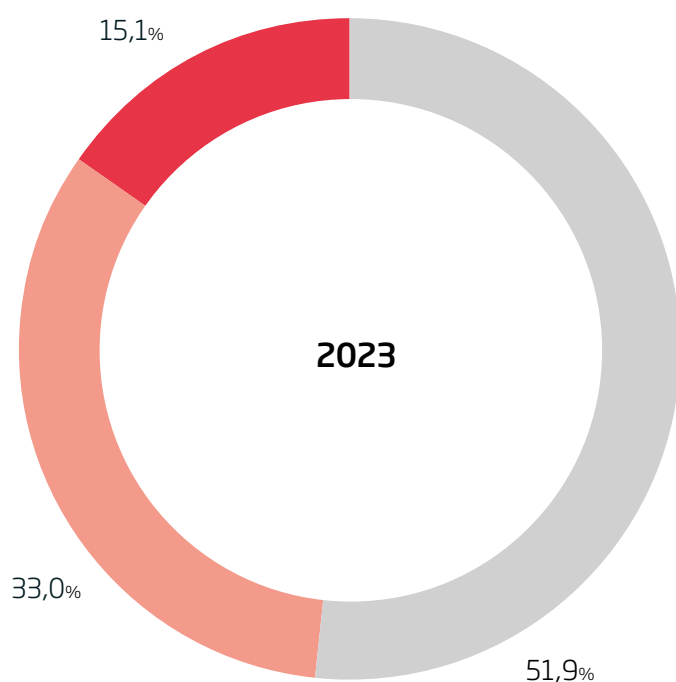
Füll- und Entleerstellen

Festgestellte Mängel bei Prüfung vor Inbetriebnahme



Füll- und Entleerstellen

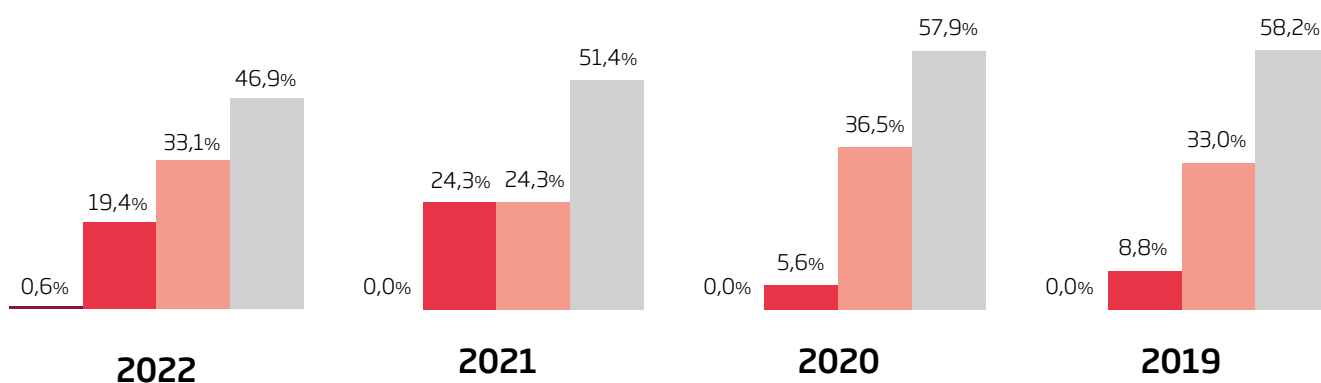
Festgestellte Mängel bei wiederkehrenden Prüfungen



51,9%

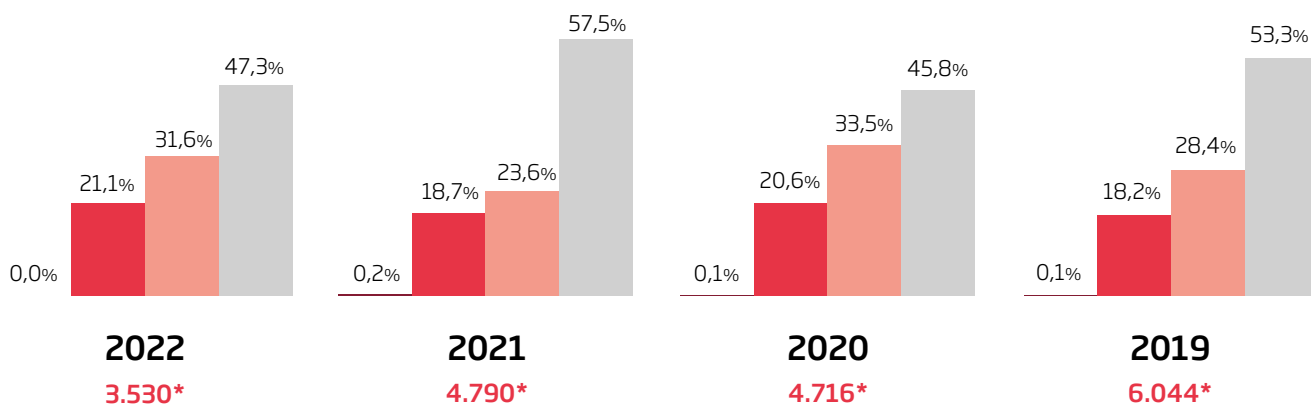
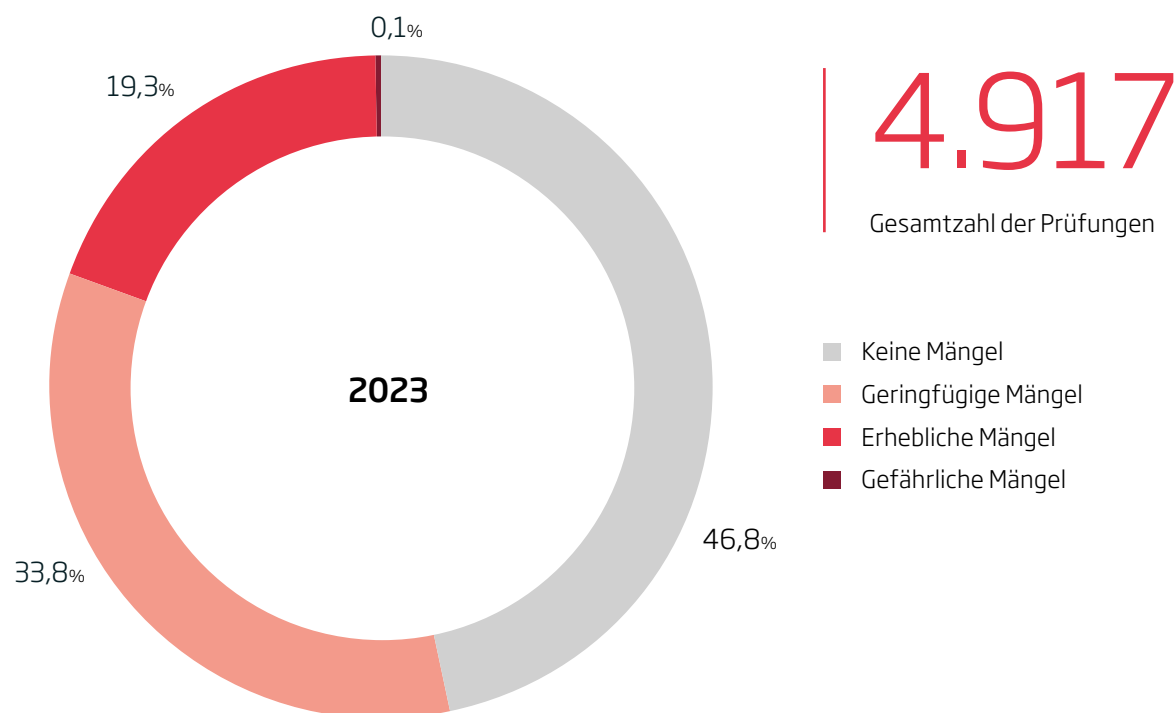
aller Füll- und Entleerstellen bei wiederkehrenden Prüfungen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



Tankstellen

Mängelverteilung über alle Prüfungen hinweg



* Gesamtzahl der Prüfungen

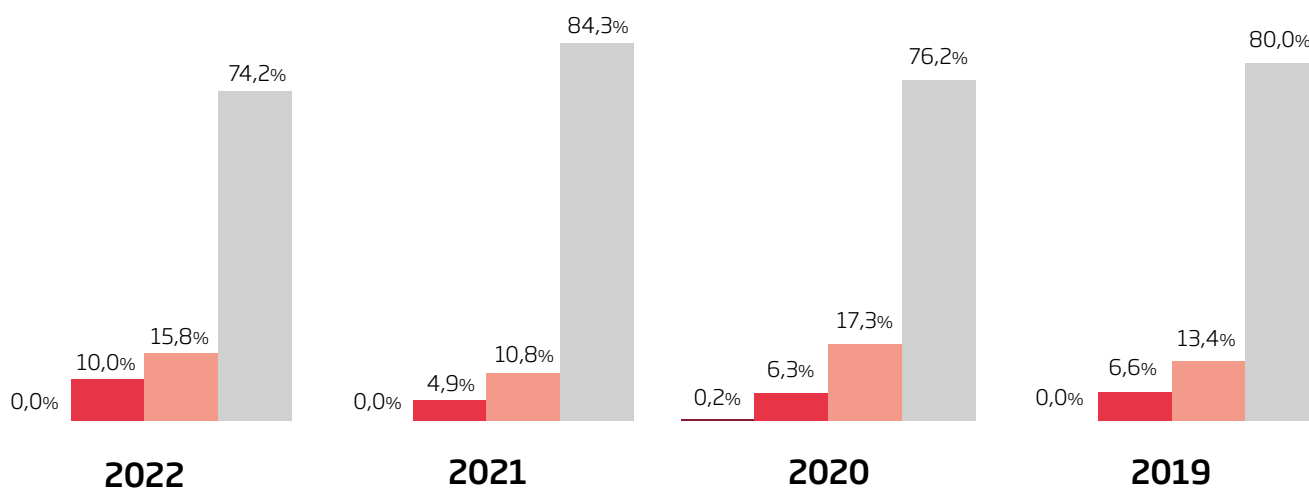
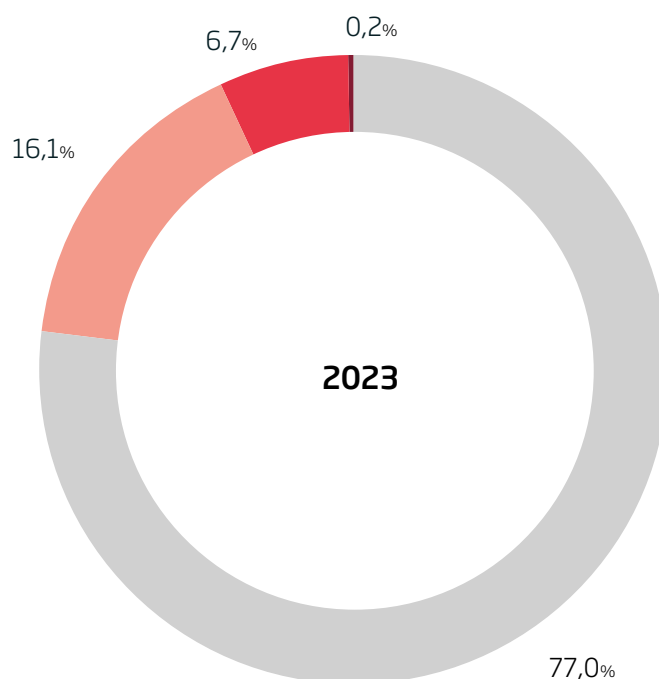
Tankstellen

Festgestellte Mängel bei Prüfung vor Inbetriebnahme

77,0%

aller vor Inbetriebnahme geprüften
Tankstellen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



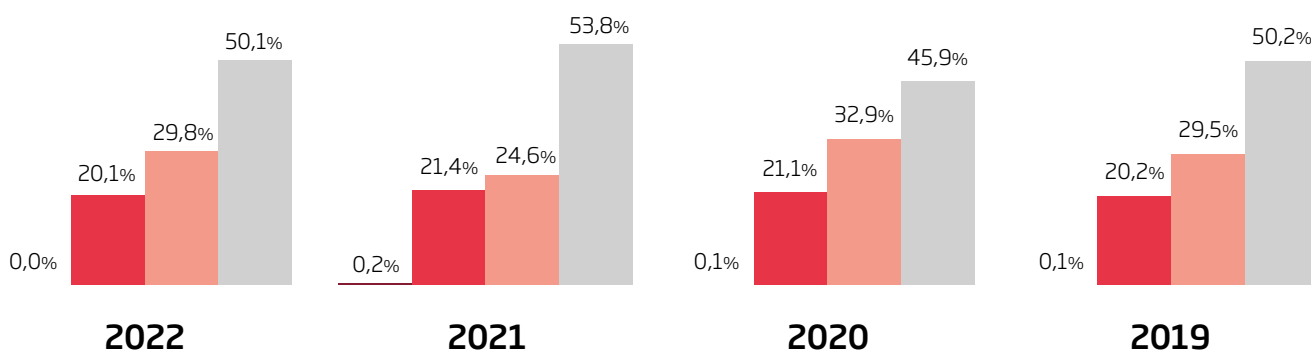
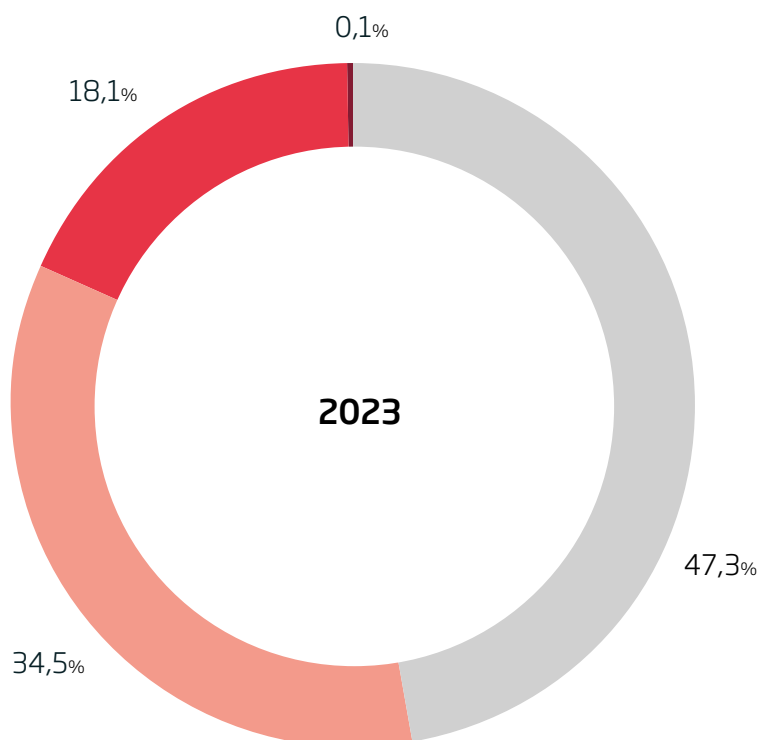
Tankstellen

Festgestellte Mängel bei wiederkehrenden Prüfungen

47,3%

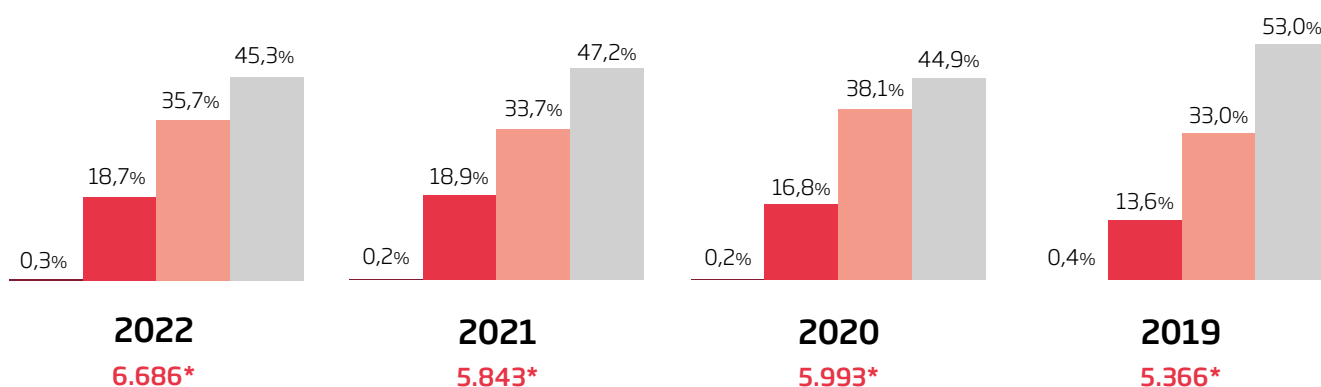
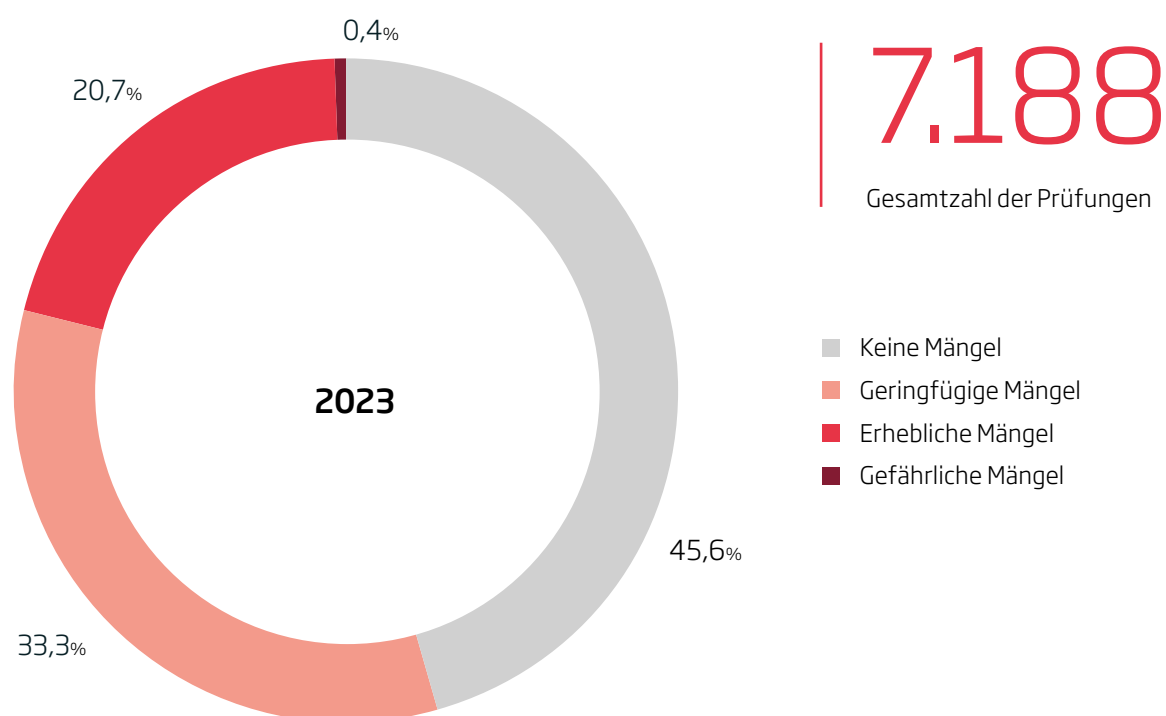
aller Tankstellen bei wiederkehrenden Prüfungen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



Sonstige Ex-Anlagen

Mängelverteilung über alle Prüfungen hinweg



* Gesamtzahl der Prüfungen

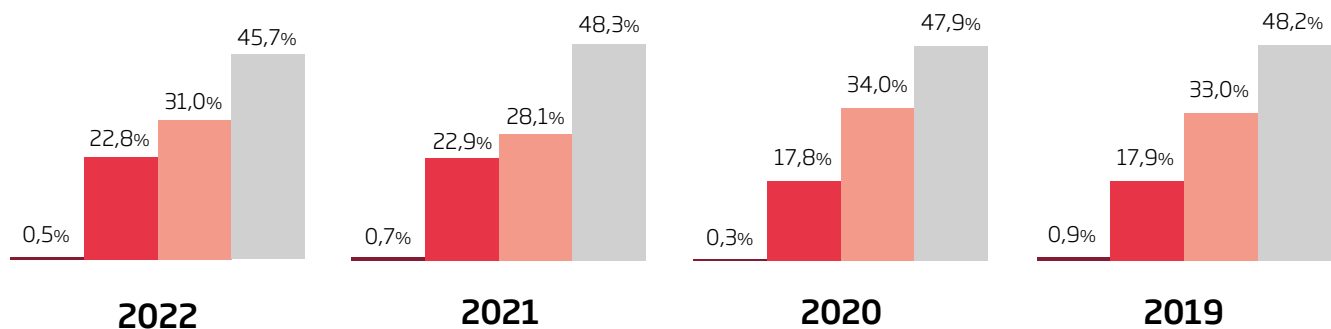
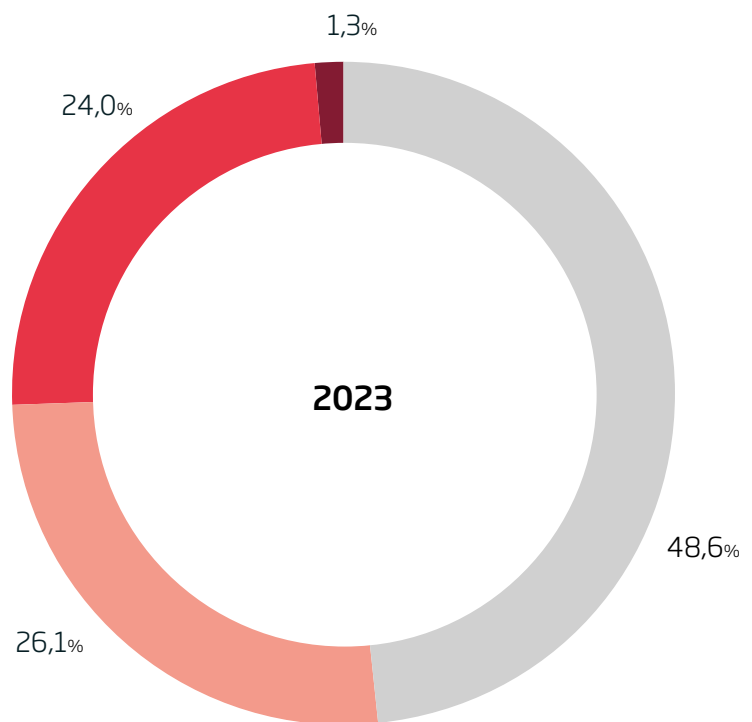
Sonstige Ex-Anlagen

Festgestellte Mängel bei Prüfung vor Inbetriebnahme

48,6%

aller vor Inbetriebnahme geprüften
Ex-Anlagen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



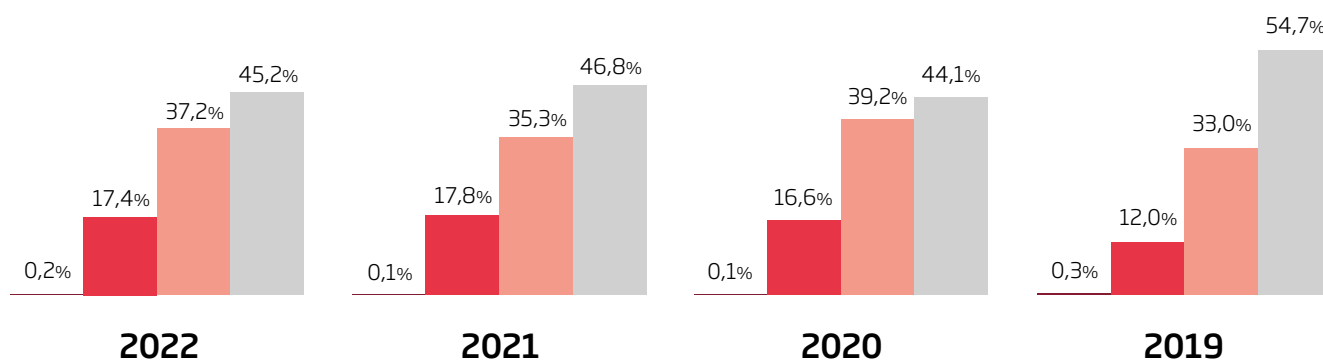
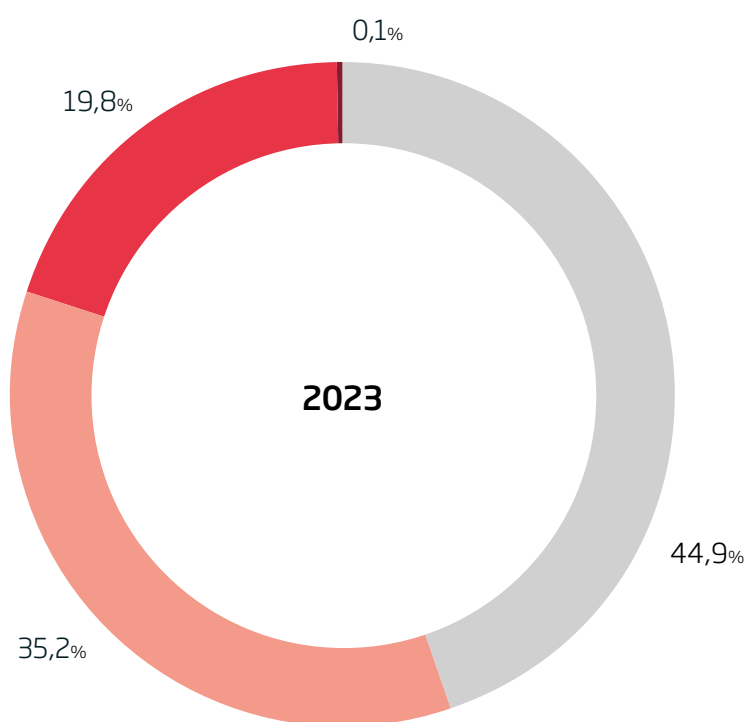
Sonstige Ex-Anlagen

Festgestellte Mängel bei wiederkehrenden Prüfungen

44,9%

aller Ex-Anlagen bei wiederkehrenden Prüfungen

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



Dokumentierte Mindestanzahl an Prüfungen, in deren Verlauf Mängel beseitigt wurden

Mängel an Ex-Anlagen, die während der Prüfung behoben werden, werden in der Statistik nicht mehr als Mängel aufgeführt. Sie sollen der Vollständigkeit halber hier aber genannt werden. Da nicht alle ZÜS die während der Prüfungen erhobenen Mängel erfassen, kann hier nur von einer dokumentierten Mindestanzahl der beseitigten Mängel geschrieben werden. Die tatsächliche Anzahl fällt höher aus.

2023

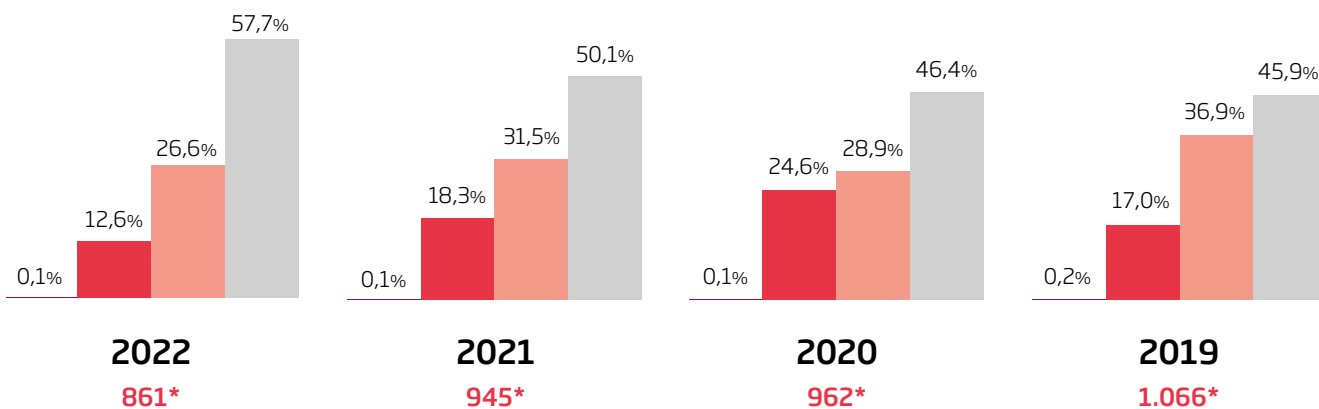
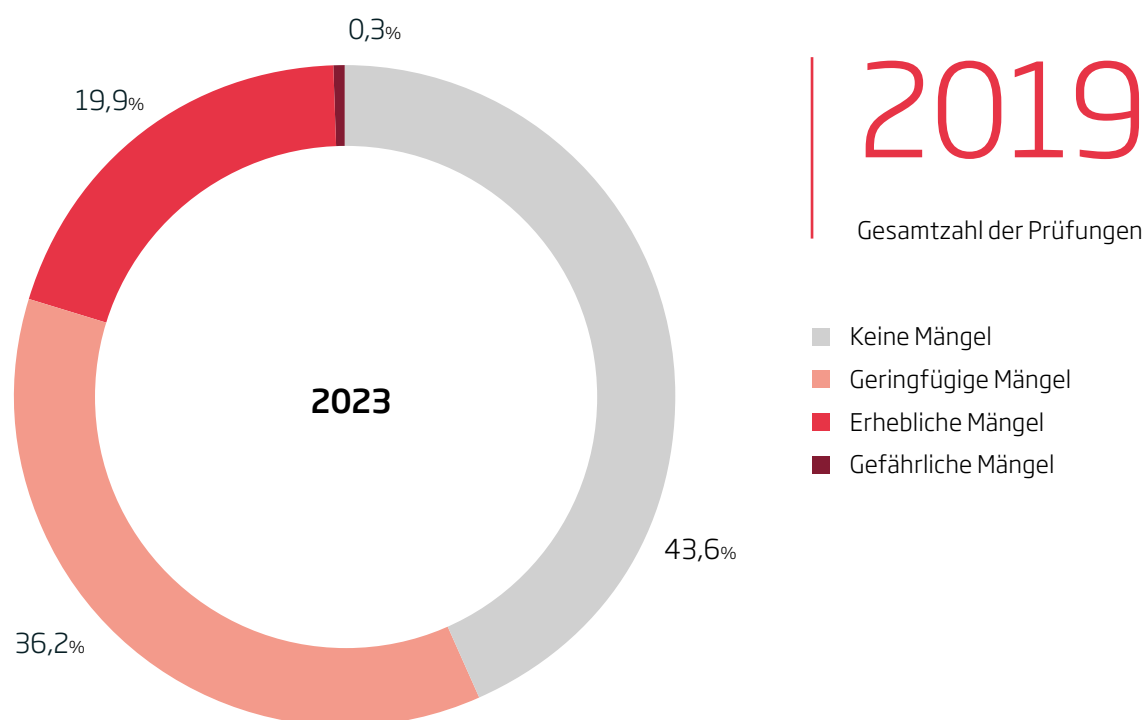
Anlagenart	Prüfung vor Inbetriebnahme	Wiederkehrende Prüfung
Lageranlagen	8	53
Füll- und Entleerstellen	2	4
Tankstellen	34	607
Sonstige Ex-Anlagen	167	526

2022 – 2019

Anlagenart	Prüfung vor Inbetriebnahme				Wiederkehrende Prüfung			
	2022	2021	2020	2019	2022	2021	2020	2019
Lageranlagen	10	8	2	2	46	29	43	54
Füll- und Entleerstellen	3	4	1	1	5	16	9	9
Tankstellen	13	9	21	25	430	443	607	1290
Sonstige Ex-Anlagen	220	160	78	46	343	361	423	203

Gasfüllanlagen

Mängelverteilung über alle Prüfungen hinweg



* Gesamtzahl der Prüfungen

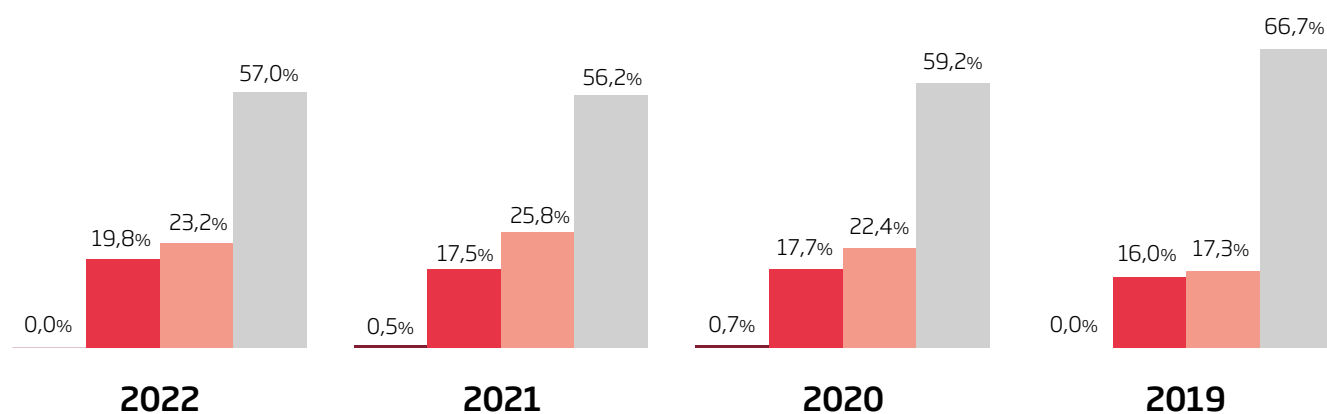
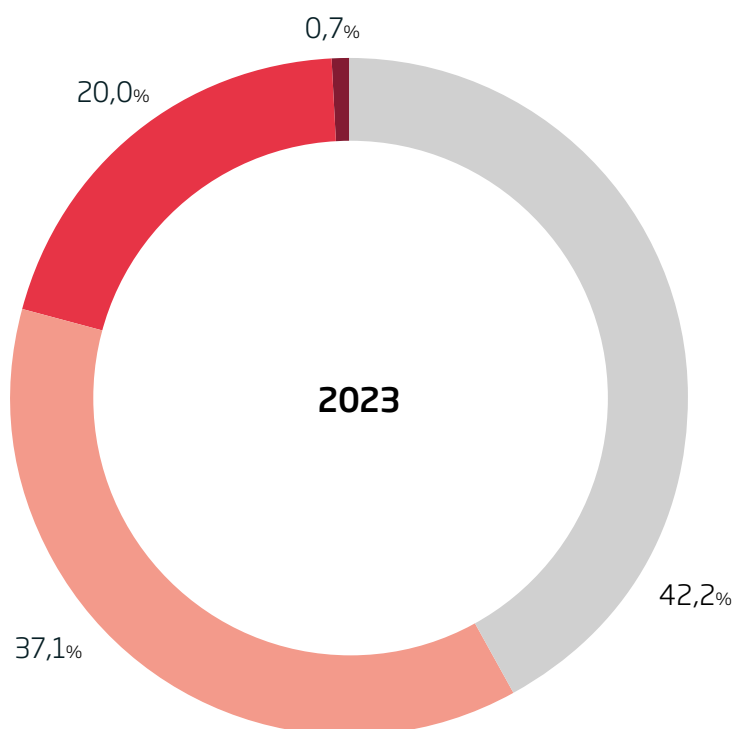
Gasfüllanlagen

Festgestellte Mängel bei Prüfung vor Inbetriebnahme

42,2%

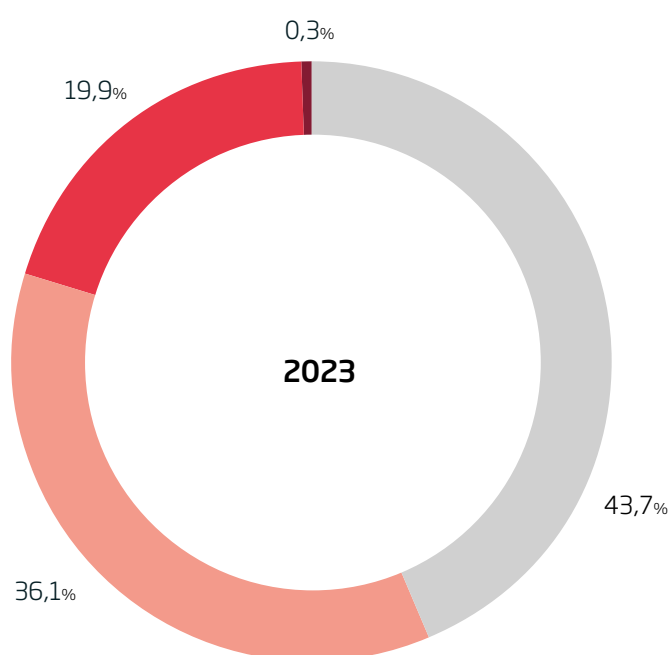
aller vor Inbetriebnahme geprüften Gasfüllanlagen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel



Gasfüllanlagen

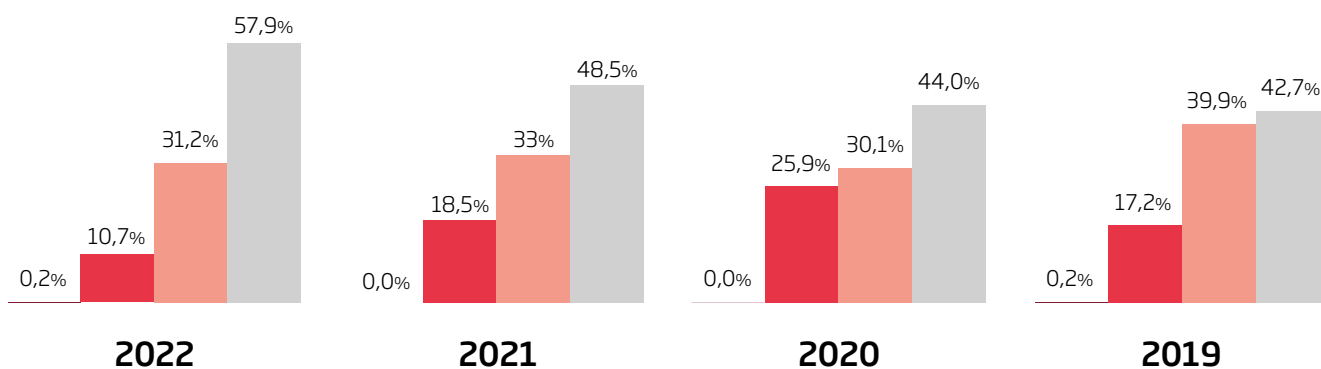
Festgestellte Mängel bei wiederkehrenden Prüfungen



43,7%

aller Gasfüllanlagen bei wiederkehrenden Prüfungen sind mängelfrei

- Keine Mängel
- Geringfügige Mängel
- Erhebliche Mängel
- Gefährliche Mängel





Die Zugelassenen Überwachungsstellen

Laut dem „Gesetz über überwachungsbedürftige Anlagen“ (ÜAnlG) dürfen nur Zugelassene Überwachungsstellen (ZÜS) die Prüfungen überwachungsbedürftiger Anlagen durchführen. Die ZÜS werden von der Zentralstelle der Länder für Sicherheitstechnik (ZLS) anerkannt. Für eine Anerkennung als ZÜS müssen Prüfstellen besonders hohe Anforderungen erfüllen. Sie müssen unter anderem unabhängig sein, über ein internes System für die Qualitätssicherung und ihre Sachverständigen über die notwendigen Kompetenzen verfügen.

Der Begriff der überwachungsbedürftigen Anlagen ist im ÜAnlG definiert. Demnach gelten Anlagen, die gewerblichen oder wirtschaftlichen Zwecken dienen oder durch die Beschäftigte gefährdet werden können, als überwachungsbedürftig. Das ist immer dann der Fall, wenn von den Anlagen im Betrieb erhebliche Risiken für die Sicherheit und die Gesundheit der Beschäftigten ausgehen können. Welche Anlagen konkret unter diesen Begriff fallen,

ist in einer Rechtsverordnung bestimmt. Aktuell gibt dies die Betriebssicherheitsverordnung vor. Die in der Verordnung genannten Anlagen müssen regelmäßig wiederkehrend, also in bestimmten Zeitabständen, von einer ZÜS geprüft werden. Hinzu kommen Prüfungen vor der ersten Inbetriebnahme, vor der Wiederinbetriebnahme einer Anlage sowie nach prüfpflichtigen Änderungen. Dieses System gewährleistet die Sicherheit und den Schutz der Menschen, die sich im Gefahrenbereich überwachungsbedürftiger Anlagen befinden.

Für alle ZÜS ist ein gemeinsamer Erfahrungsaustausch vorgeschrieben. Im Erfahrungsaustauschkreis der Zugelassenen Überwachungsstellen (EK ZÜS) tauschen sich die Mitglieder fachlich aus und teilen Erkenntnisse aus ihrer Prüftätigkeit, um Schadensfälle in Zukunft zu verhindern. Der EK ZÜS hat drei ständige Arbeitskreise für die Tätigkeitsbereiche Druckanlagen, Aufzugsanlagen sowie Anlagen in explosionsgefährdeten Bereichen eingerichtet.

Adressen der beteiligten ZÜS

DEKRA Automobil GmbH

Handwerkstraße 15
70565 Stuttgart
Tel.: +49 (0)711 7861-0
Fax: +49 (0)711 7861-2240
info@dekra.com
www.dekra.com

DEKRA Testing and Certification GmbH

Dinnendahlstraße 9
44809 Bochum
Tel.: +49 (0)234-3 69 60
Fax: +49 (0)234-3 69 61 11
dtc-zues@dekra.com
www.dekra-testing-and-certification.de

GTÜ Anlagensicherheit GmbH

Vor dem Lauch 25
70567 Stuttgart
Tel.: +49 (0)711 97676-740
Fax: +49 (0)711 97676-749
info@gtue.de
www.gtue.de

SGS-TÜV Saar GmbH

Am TÜV 1
66280 Sulzbach
Tel.: +49 (0)6897 506-60
Fax: +49 (0)6897 506-102
info@sgs-tuev.de
www.sgs-tuev-saar.com

TÜV Austria Services GmbH

Kurze Straße 40
70794 Filderstadt
Tel.: +49 (0)711 722 336 22
tuv-deutschland@tuv.at
www.tuv-ad.de

TÜV NORD Systems GmbH & Co. KG

Große Bahnstraße 31
22525 Hamburg
Tel.: +49 (0)40 8557-0
Fax: +49 (0)40 8557-2295
info@tuev-nord.de
www.tuev-nord.de

TÜV Rheinland Industrie Service GmbH

Am Grauen Stein
51105 Köln
Tel.: +49 (0)221 806-0
Fax: +49 (0)221 806-1753
industrie-service@de.tuv.com
www.tuv.com

TÜV SÜD Chemie Service GmbH

Kaiser-Wilhelm-Allee, Geb. B 407
51368 Leverkusen
Tel.: +49 (0)214 86910-0
Fax: +49 (0)214 86910-296
vertrieb.chemieservice@tuvsud.com
www.tuvsud.com/chemieservice

TÜV SÜD Industrie Service GmbH

Westendstraße 199
80686 München
Tel.: +49 (0)89 5791-0
Fax: +49 (0)89 5791-1551
info@tuvsud.com
www.tuvsud.com/de-is

TÜV Technische Überwachung Hessen GmbH

Robert-Bosch-Straße 16
64293 Darmstadt
Tel.: +49 (0)6151 600-0
Fax: +49 (0)6151 600-600
mailbox@tuevhessen.de
www.tuev-hessen.de

TÜV Thüringen e. V.

Melchendorfer Straße 64
99096 Erfurt
Tel.: +49 (0)361 42 83-0
Fax: +49 (0)361 42 83-242
info@tuev-thueringen.de
www.tuev-thueringen.de

Herausgeber

TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin
Tel.: +49 (0)30 760095-400
E-Mail: berlin@tuev-verband.de
www.tuev-verband.de
www.twitter.com/tuevverband

Verantwortlich

Dr. Joachim Bühler

Redaktion

Eike Brand
Dr. Hermann Dinkler
Fee Hovehne
André Siegl
Maurice Shahd
Claudia Tautorus

Bildnachweis

S. 1 – © AdobeStock
S. 5 – © Tobias Koch
S. 8 – © Dieter Roas/TÜV SÜD
S. 9 – © Viktor Kiryanov/unsplash
S. 15 – © AdobeStock
S. 17 – © Pierre Chatel Innocenti
S. 19 – © Freepik
S. 21 – © Steimers
S. 22 – © AdobeStock
S. 28 – © The Blowup/unsplash
S. 36 – © Khamkeo Vilaysing-/unsplash
S. 54 – © Freepik