

Warum Softwaresicherheit bei mobilen Lichtsignalanlagen unerlässlich ist

Bei mobilen Lichtsignalanlagen (LSA) wird in der Praxis häufig über Standsicherheit, Anzahl und Ausbau von Signalgebern sowie deren Aufstellorte gesprochen. Diese Aspekte sind zweifellos wichtig. Auffällig ist jedoch, dass der zweite sicherheitsrelevante Kernbereich – neben der Sicherheit der Hardware – oftmals deutlich weniger Beachtung findet: die Softwaresicherheit.

Von LSA – insbesondere von mobilen – wird erwartet, dass sie „einfach funktionieren“. Dabei ist gerade dieser Nachweis der Softwaresicherheit im Ernstfall von zentraler Bedeutung: technisch, zivilrechtlich und nicht zuletzt strafrechtlich.

Lichtsignalanlagen als sicherheitsrelevante Systeme

LSA sind sicherheitsrelevante Systeme und Teil der kritischen Infrastruktur. Sie greifen unmittelbar in den Straßenverkehr ein und beeinflussen das Verhalten von Verkehrsteilnehmern maßgeblich. Nicht zuletzt verlassen sich diese teilweise blind auf die Richtigkeit des angezeigten Signalbilds.

Fehlerhafte Signalbilder, widersprüchliche Freigaben oder unkontrollierte Zustandswechsel können daher unmittelbar zu Unfällen mit erheblichen Perso-

nen- und Sachschäden führen.

Die LSA muss folglich jederzeit in der Lage sein, alle geschalteten Zeiten und Zustandswechsel zu überwachen und zu analysieren. Nur so können fehlerhafte Zustände erkannt und verhindert werden. Hierfür gibt es in jedem Steuergerät eine Signalisierungseinrichtung. Sie ist das Herzstück einer LSA und überwacht sämtliche Schaltungen auf ihre Korrektheit. Bspw. muss sie beim Erkennen eines gefährlichen Zustands die LSA innerhalb von 300 ms sicher abschalten.

Der unterschätzte Faktor Software

Es muss nachweisbar sichergestellt und dokumentiert werden, dass die LSA wirklich bei jeglichen Fehlern eigensicher arbeiten wird – bezogen auf die Hardware und ganz besonders auf die Software.

In der Praxis wird Software jedoch häufig als „ausreichend sicher“ betrachtet, solange die Anlage im Alltag scheinbar problemlos funktioniert. Solange sie schaltet, keine offensichtlichen Fehlfunktionen zeigt und bis-

lang kein Unfall passiert ist, gilt das System als unproblematisch. Dieses Verständnis greift zu kurz, denn ein störungsfreier Betrieb ist kein Sicherheitsnachweis.

Normative Anforderungen an die Softwaresicherheit

Die Aufgabe der Normgebung ist es, einen einheitlichen Standard zu schaffen, um genau diesem Problem entgegenzuwirken. Diese Funktion erfüllt die DIN VDE V 0832-500:2016-10. Sie fordert, dass gefährliche Zustände systematisch ausgeschlossen werden müssen. Dies betrifft nicht nur die Hardware, sondern insbesondere die Software als steuerndes Element.

Logik, Zustandsautomaten, Fehlerbehandlung, Prioritäten und Reaktionen auf Störungen sind so zu gestalten, dass auch bei internen Fehlern oder äußeren Einflüssen kein unzulässiges Signalbild angezeigt werden kann.

Software ist damit kein bloßes Funktionsmittel, sondern ein zentrales sicherheitsrelevantes Element der Gesamtanlage!

Sicherheit bedeutet mehr als störungsfreien Betrieb

Sicherheit im normativen Sinne bedeutet nicht, dass bisher nichts passiert ist, sondern dass Risiken systematisch identifiziert, bewertet und beherrscht werden.

Ohne einen dokumentierten Nachweis der Softwaresicherheit bleibt unklar, ob die Steuerungsoftware deterministisch arbeitet, ob alle relevanten Fehlerzustände berücksichtigt wurden, ob definierte sichere Zustände existieren und ob die LSA überhaupt dafür geeignet ist, maßgeblich in den Straßenverkehr eingreifen zu dürfen.



Nicht nur die Hardware einer LSA muss sicher funktionieren, auch der Nachweis der Softwaresicherheit ist im Ernstfall von zentraler Bedeutung: technisch, zivilrechtlich und nicht zuletzt strafrechtlich

Verfasser

Julien Hasenburg
julien.hasenburg@fabema.de

FABEMA GmbH
D-51515 Kürten
www.fabema.de

Besonders kritisch sind Situationen außerhalb des Normalbetriebs, etwa Spannungsunterbrechungen, Kommunikationsfehler, Speicherfehler, fehlerhafte Initialisierungen oder das Wiederanlaufen nach Störungen. Gerade in diesen Fällen entscheidet die Software darüber, ob die Anlage kontrolliert in einen sicheren Zustand übergeht oder unkontrolliert reagiert.

Verantwortung und Haftungsfragen

Kommt es in einer o. g. Situation zu einem Unfall, rückt die Frage der Verantwortung unweigerlich in den Mittelpunkt. Dann genügt es nicht, auf eine CE-Kennzeichnung, auf Normen für die elektrotechnische Ausführung oder auf einen bislang unauffälligen Betrieb zu verweisen. Maßgeblich ist vielmehr, ob der Stand der Technik eingehalten und die in der DIN VDE V 0832-500:2016-10 be-

schriebenen Sicherheitsprinzipien nachweislich umgesetzt wurden.

Fehlt dieser Nachweis, entsteht schnell der Vorwurf, mögliche Risiken nicht ausreichend analysiert und berücksichtigt zu haben. Auch wenn es sich um eine Vornorm handelt, ist ihre Bedeutung keineswegs nachrangig. Vornormen bilden den anerkannten Stand der Technik ab – insbesondere dann, wenn sie die einzige oder aktuell konkretisierende Regelung für ein Themenfeld darstellen.

Im Haftungs- und Strafrecht kommt es nicht auf den formalen Status einer Norm an, sondern darauf, ob sie geeignet ist, den Stand der Technik sachgerecht zu beschreiben.

Organisatorische und strafrechtliche Relevanz

Besonders brisant ist, dass sich die Verantwortung nicht auf eine

einzelne Stelle beschränkt. Je nach Konstellation können Hersteller, Inverkehrbringer, Betreiber sowie weitere verantwortliche Personen in den Fokus geraten.

Strafrechtlich relevant werden dabei insbesondere Fragen der Fahrlässigkeit. Wer ein sicherheitsrelevantes System betreibt oder in Verkehr bringt, muss geeignete organisatorische und technische Maßnahmen treffen, um Gefahren zu vermeiden. Der fehlende Nachweis der Software-sicherheit kann dabei als Indiz gewertet werden, dass diese Pflicht systematisch und vorsätzlich verletzt wurde.

Die DIN VDE V 0832-500:2016-10 verlangt ausdrücklich keine fehlerfreie Software. Gefordert wird vielmehr eine systematische Beherrschung von Fehlern. Dazu gehören u. a. klar definierte sichere Zustände, eindeutige Prioritäten, nachvollziehbare Programmstrukturen, dokumentierte Test-

szenarien sowie eine vollständige, fachmännisch geprüfte technische Dokumentation einschließlich der erforderlichen Organisationsstruktur. Nur so lässt sich im Nachhinein belegen, dass Risiken erkannt und mit angemessener Sorgfalt behandelt wurden.

Fazit

Der Nachweis der Softwaresicherheit ist kein formaler Akt und kein „Papier für die Akte“. Er ist ein zentrales Instrument der Risikoversorge. Wer ihn ernst nimmt, schützt nicht nur Verkehrsteilnehmer, sondern auch sich selbst und alle weiteren Beteiligten. Im Schadensfall kann er entscheidend dafür sein, ob ein Ereignis als unvermeidbarer Unfall oder als vermeidbare Pflichtverletzung bewertet wird. ■