INB 2027 (neu)	Begründung für die unterjährige Änderung
Die Regelungen zur Ausnahme 255 zur Ril 408 entnehmen Sie bitte dem Regelwerksdokument.	Hintergrund für die unterjährige Änderung ist, dass zum Zeitpunkt der Veröffentlichung der Ril 408.2412 die Betriebserprobung des Digitalen Befehls auf der SFS Wendlingen-Ulm noch im Gange war bzw. die bundesweite Betriebserprobung noch nicht gestartet war. Durch die Ausnahme können die Erkenntnisse, Erfahrungen und Anwenderrückmeldungen aus der bundesweiten Betriebserprobung in das Regelwerk einfließen. Die Ausnahme ist erforderlich, um die Übermittlungsart Digitaler Befehl in den Regelbetrieb zu überführen. Sie enthält folgende geänderte Richtlinie: • 408.2412 • 408.0055 Wir beabsichtigen, die Regeln der Ausnahme 255 voraussichtlich im Rahmen der Aktualisierung 2 in die Richtlinienfamilie 408 zu überführen.

Abschn./ Pkt	Regelung alt	Regelung neu	Änderungsgrund/ Anmerkungen
408.2412 2.3	**2.3 Übermitteln, Rückfallebene und eindeutige Kennung** **Übermitteln** Der Fdl erteilt mit der Anwendung „Digitaler Befehl“ Befehle an Tf. **Rückfallebene** Bei einer Fehlfunktion der Anwendung oder wenn der Tf den Befehl nicht digital abrufen kann, ist der Fdl zu verständigen. **Eindeutige Kennung** Jede Befehlsnachricht ist mit einer eindeutigen Kennung gekennzeichnet. Diese setzt sich zusammen aus einer Abkürzung gemäß Streckenbuch EIU, einer laufenden vierstelligen Nummer und der Zugnummer des Zuges, dem die Befehlsnachricht erteilt wird.	**2.3 Übermitteln, Rückfallebene und eindeutige Kennung** **Übermitteln** Der Fdl erteilt mit der Anwendung „Digitaler Befehl“ Befehle an Tf. Der Digitale Befehl ist das Standardübermittlungsverfahren für Befehle. Auf Anfrage des Fdl muss der Tf mitteilen, ob der Zug signalgeführt, LZB-geführt oder ETCS-geführt ist. Bei ETCS muss er dem Fdl zusätzlich mitteilen, in welchem ETCS-Level und in welcher ETCS-Betriebsart sich der Zug befindet. Sollte sich die Zugbeeinflussung zwischen dem Zeitpunkt der Mitteilung an den Fdl und dem Abruf einer Befehlsnachricht ändern, muss der Tf dies dem Fdl mitteilen. **Rückfallebene Digitaler Befehl** Bei einer Fehlfunktion der Anwendung oder wenn der Tf den Befehl nicht digital abrufen oder quittieren kann, ist der Fdl zu verständigen. Falls ein gültiger Befehl in der Anwendung nicht mehr einsehbar ist oder nicht korrekt dargestellt wird, muss der Tf den Zug sofort anhalten und nach dem Anhalten den Fdl verständigen. **Eindeutige Kennung** Jede Befehlsnachricht ist mit einer eindeutigen Kennung gekennzeichnet. Diese setzt sich zusammen aus einer Abkürzung gemäß Streckenbuch EIU, einer laufenden vierstelligen Nummer und der Zugnummer des Zuges, dem die Befehlsnachricht erteilt wird.	**Übermitteln** Der Digitale Befehl wird als standardmäßige Übermittlungsmethode hinzugefügt. Analog zur Befehlsübermittlung gemäß Ril 408.2411 muss der Tf auf Anfrage des Fdl die Zugbeeinflussung nennen. Weiterhin wurde ergänzt, dass der Tf eine Änderung der Zugbeeinflussung vor Abruf der Befehlsnachricht mitteilen muss. **Rückfallebene** Hierbei wird eine neue Regelung eingeführt, falls ein gültiger Digitaler Befehl nicht mehr einsehbar ist bzw. nicht korrekt dargestellt wird. Dieser Fall eines Darstellungsfehlers wurde im Rahmen der CSM-RA zum Digitalen Befehl behandelt.

408.2412 2.4	**2.4 Abruf der Befehlsnachricht** **Voraussetzungen** Die Befehlsnachricht darf nur bei Halt des Zuges abgerufen werden. **Zugriffscode** Für den Abruf der Befehlsnachricht wird ein Zugriffscode benötigt. Der Zugriffscode wird in der Regel per SMS an das GSM-R Zugfunk-Fahrzeuggerät gesendet. Im Falle einer gestörten Zustellung des Zugriffscodes, ist der Fdl zu verständigen. Dieser teilt dem Tf den Zugriffscode mündlich mit. Bei Schichtübergabe zu einem übernehmenden Tf ist diesem der Zugriffscode zu übergeben bzw. darauf hinzuweisen, sofern eine Befehlsnachricht weiterhin Gültigkeit besitzt. Der übernehmende Tf führt im Falle, dass er ein persönliches Endgerät besitzt, einen Folgeabruf auf diesem durch. **Meldung von Standort und Zugbeeinflussung** Um Einsicht in die Befehlsnachricht zu erhalten, muss der Tf den Standort des Zuges eingeben. Hierbei sind Signalbezeichnungen zu verwenden. Ist das nicht möglich, ist der km der Spitze des Zuges oder die Weichenbezeichnung anzugeben. Zusätzlich muss der Tf mitteilen, ob der Zug signalgeführt, LZB-geführt oder ETCS-geführt ist. Bei ETCS muss er dem Fdl zusätzlich mitteilen, in welchem ETCS-Level und in welcher ETCS-Betriebsart sich der Zug befindet. **Verständigen** Der Tf des Fahrzeugs an der Spitze des Zuges muss den Tb vom Inhalt eines Befehls unterrichten und für die Unterrichtung der anderen Tf sorgen, wenn der Inhalt des Befehls für das Verhalten der Tf Bedeutung hat.	**2.4 Abruf der Befehlsnachricht** **Voraussetzungen** Die Befehlsnachricht darf nur bei Halt des Zuges abgerufen werden. **Zugriffscode** Für den Abruf der Befehlsnachricht wird ein Zugriffscode benötigt. Der Zugriffscode wird in der Regel per SMS an das GSM-R Zugfunk-Fahrzeuggerät gesendet. Im Falle einer gestörten Zustellung des Zugriffscodes, ist der Fdl zu verständigen. Dieser teilt dem Tf den Zugriffscode mit. Bei Schichtübergabe zu einem übernehmenden Tf ist diesem der Zugriffscode zu übergeben bzw. darauf hinzuweisen, sofern eine Befehlsnachricht weiterhin Gültigkeit besitzt. Der übernehmende Tf führt im Falle, dass er ein persönliches Endgerät besitzt, einen Folgeabruf auf diesem durch. **Standortmeldung** Um Einsicht in die Befehlsnachricht zu erhalten, muss der Tf den Standort des Zuges eingeben. Hierbei sind Signalverwendung und -bezeichnung zu verwenden. Ist das nicht möglich, ist der km der Spitze des Zuges oder die Weichenbezeichnung anzugeben. **Verständigen** Der Tf des Fahrzeugs an der Spitze des Zuges muss den Tb vom Inhalt eines Befehls unterrichten und für die Unterrichtung der anderen Tf sorgen, wenn der Inhalt des Befehls für das Verhalten der Tf Bedeutung hat.	**Standortmeldung** Um eine prozessual richtige Reihenfolge der Meldungen zu schaffen, wurde hier die Meldung der Zugbeeinflussung entfernt.

Abschn./ Pkt	Regelung alt	Regelung neu	Änderungsgrund/ Anmerkungen
408.2412 2.5	**2.5 Handhaben durch den Tf** - Nachdem der Tf eine Befehlsnachricht abgerufen hat, muss er prüfen, ob sich der Inhalt der Befehlsnachricht auf seinen Zug und dessen Standort bezieht. Der Tf muss alle in der Befehlsnachricht enthaltenen Befehle lesen, prüfen und als gelesen markieren. - Wenn die Prüfung nicht erfolgreich abgeschlossen werden kann, muss der Tf die Befehlsnachricht abweisen und den Fdl mündlich verständigen. - Wenn alle Befehle als gelesen markiert sind, muss der Tf die Befehlsnachricht quittieren. Erst mit der erfolgreichen Quittierung wird die Befehlsnachricht gültig. - Der Tf muss sicherstellen, dass die Befehle bis zur Erledigung im Führerraum auf dem Endgerät angezeigt werden. Wenn der Tf sich nicht im Führerraum aufhält, muss er das Endgerät mit den Befehlen bei sich führen. Sofern dies nicht möglich ist, muss er sich die Befehle mit Vordruck 408.2411V01 vom Fdl übermitteln lassen. - Wenn der Tf das Fahrzeug an der Spitze des Zuges wechselt oder ein Personalwechsel stattfindet, muss der Tf für die Übergabe weiterhin gültiger Befehle sorgen. Sofern persönliche Endgeräte verwendet werden, muss der übergebende Tf dem übernehmenden Tf den erforderlichen Zugriffscode und die eindeutige Kennung nach Absatz 2.2 mitteilen. Der übernehmende Tf muss die Befehlsnachrichten nach Absatz 2.3 abrufen. Sofern dies nicht möglich ist, muss er sich die Befehle mit Vordruck 408.2411V01 vom Fdl übermitteln lassen. - Eine Befehlsnachricht muss der Tf als erledigt markieren, wenn alle enthaltenen Befehle abgearbeitet sind.	**2.5 Handhabung durch den Tf** Nachdem der Tf eine Befehlsnachricht abgerufen hat, muss er prüfen, ob sich der Inhalt der Befehlsnachricht auf seine Zugnummer und dessen Standort bezieht. Der Tf muss alle in der Befehlsnachricht enthaltenen Befehle lesen und als gelesen markieren. Wenn alle Befehle als gelesen markiert sind, muss der Tf die Befehlsnachricht quittieren. Mit der Quittierung bestätigt der Tf, dass er den Inhalt der Befehlsnachricht verstanden hat und die Befehle zur Ausführung akzeptiert. Erst mit der erfolgreichen Quittierung wird die Befehlsnachricht gültig. Wenn die Prüfung nicht erfolgreich abgeschlossen werden kann, muss der Tf die Befehlsnachricht abweisen und den Fdl verständigen. Der Tf muss sicherstellen, dass die Befehle bis zur Erledigung im Führerraum auf dem Endgerät angezeigt werden. Wenn der Tf sich nicht im Führerraum aufhält, muss er das Endgerät mit den Befehlen mit sich führen. Sofern dies nicht möglich ist, muss er sich die Befehle gemäß Ril 408.2411 vom Fdl übermitteln lassen. Wenn der Tf das Fahrzeug an der Spitze des Zuges wechselt oder ein Personalwechsel stattfindet, muss der Tf für die Übergabe weiterhin gültiger Befehle sorgen. Wenn persönliche Endgeräte verwendet werden, muss der übergebende Tf dem übernehmenden Tf den erforderlichen Zugriffscode und die eindeutige Kennung nach Absatz 2.3 mitteilen. Der übernehmende Tf muss die Befehlsnachrichten nach Absatz 2.4 abrufen. Wenn dies nicht möglich ist, muss er sich die Befehle gemäß Ril 408.2411 vom Fdl übermitteln lassen. Eine Befehlsnachricht muss der Tf als erledigt markieren, wenn alle enthaltenen Befehle abgearbeitet sind.	Der Begriff „Zug“ wurde mittels „Zugnummer“ präzisiert. Das Wort „prüfen“ war nicht eindeutig und wurde durch eine Formulierung ersetzt, dass der Tf mit der Quittierung bestätigt, dass er den Inhalt der Befehlsnachricht verstanden hat und ausführen wird. Weiterhin wurden redaktionelle Anpassungen vorgenommen zum besseren Verständnis der Regelungen.

<table>
<tr><th>Abschn./
Pkt</th><th>Regelung alt</th><th>Regelung neu</th><th>Änderungsgrund/
Anmerkungen</th></tr>
<tr>
<td>408.2412 2.6</td>
<td>
2.6 Befehl widerrufen
Für das Widerrufen von Befehlen gilt:
<table>
<tr><th>Befehl</th><th>Widerrufen durch</th><th>Besonderheiten</th></tr>
<tr><td>Alle</td><td>Befehl 4</td><td>Wenn mehrere Befehle in einer Befehlsnachricht erteilt wurden, müssen alle Befehle widerrufen werden.</td></tr>
<tr><td>3</td><td>Befehle 1, 2 oder 7</td><td>Kein Befehl 4 erforderlich.

Wurde Befehl 3 als Befehlsnachricht übermittelt, ist zusätzlich Befehl 95 mit Auftrag 95.95 mit folgendem Wortlaut zu erteilen:
„Befehl mit … [Eindeutige Kennung der widerrufenen Befehlsnachricht] ist als manuell widerrufen zu markieren.“</td></tr>
</table>
- Wird ein Befehl 3 mit Befehl 1, 2 oder 7 widerrufen, so ist der widerrufene Befehl in der Anwendung manuell als widerrufen zu markieren.
- Kann die Befehlsnachricht nicht digital widerrufen werden, wird diese durch den Fdl über den Vordruck 408.2411V01 gem. Ril 408.2411 widerrufen. Die widerrufene Befehlsnachricht ist durch den Tf als manuell widerrufen zu kennzeichnen.
- Wenn ein Befehl widerrufen wurde und wenn der Zug seine Fahrtrichtung ändert oder das Fahrzeug an der Spitze des Zuges wechselt oder ein anderer Tf die Arbeit übernimmt, ist ergänzend zu den Regeln in Absatz 2.4 der mit Vordruck 408.2411V01 erteilte Befehl 4 bzw. 1, 2 oder 7 zu übergeben. Die widerrufene Befehlsnachricht darf nicht erneut abgerufen werden.
</td>
<td>
2.6 Befehl widerrufen
Für das Widerrufen von Befehlen gilt:
<table>
<tr><th>Befehl</th><th>Widerrufen durch</th><th>Besonderheiten</th></tr>
<tr><td>Alle</td><td>Befehl 4</td><td>Wenn mehrere Befehle in einer Befehlsnachricht erteilt wurden, müssen alle Befehle widerrufen werden.</td></tr>
</table>
Kann die Befehlsnachricht nicht digital widerrufen werden, wird diese durch den Fdl über den Vordruck 408.2411V01 gem. Ril 408.2411 widerrufen. Die widerrufene Befehlsnachricht ist durch den Tf als manuell widerrufen zu kennzeichnen.
Wenn ein Befehl widerrufen wurde und wenn der Zug seine Fahrtrichtung ändert oder das Fahrzeug an der Spitze des Zuges wechselt oder ein anderer Tf die Arbeit übernimmt, ist ergänzend zu den Regeln in Absatz 2.5 der mit Vordruck 408.2411V01 erteilte Befehl 4 bzw. 1, 2 oder 7 zu übergeben. Die widerrufene Befehlsnachricht darf nicht erneut abgerufen werden.
</td>
<td>
Die bisherige Regelung, nach der ein Befehl 3 durch die Befehle 1, 2 oder 7 ohne Verwendung eines Befehls 4 widerrufen werden konnte, wurde aufgehoben. Hintergrund ist, dass die Anwendung „Digitaler Befehl“ ohne einen Befehl 4 keine eindeutige Verknüpfung zu der zu widerrufenden Befehlsnachricht herstellen kann. In der Betriebserprobung war daher vorgesehen, dass sowohl der Fdl als auch der Tf einen Befehl 3 nach einem solchen Widerruf manuell als widerrufen kennzeichnen mussten.

Auf Basis des erhaltenen Feedbacks und des Wunsches, den manuellen Widerruf in diesem Fall entfallen zu lassen, wurde die Regelung angepasst. Zukünftig muss ein Widerruf des Befehls 3 durch den Befehl 4 erfolgen. Der Fdl kann dabei in derselben Befehlsnachricht neben dem Befehl 4 gleichzeitig die Befehle 1, 2 oder 7 erteilen.
</td>
</tr>
</table>

			Durch den Befehl 4 wird die ursprüngliche Befehlsnachricht mit dem Befehl 3 automatisch als widerrufen gekennzeichnet. Eine zusätzliche manuelle Markierung durch Fdl und Tf ist damit nicht mehr erforderlich.
408.0055 2 Befehls-nachricht	Befehlsnachricht: Mit einer Befehlsnachricht erhält der Tf innerhalb der IT-Anwendung „Digitaler Befehl“ einen für die Zugfahrt erforderlichen Befehl in Form einer digital übermittelten Information mit visueller Darstellung. Eine Befehlsnachricht kann mehrere für die Zugfahrt erforderliche Befehle enthalten.	**Befehlsnachricht** Mit einer Befehlsnachricht erhält der Tf innerhalb der IT-Anwendung „Digitaler Befehl“ einen vom Fdl erstellten Befehl in Form digital übermittelter Aufträge mit visueller Darstellung. Eine Befehlsnachricht kann mehrere Befehle enthalten.	Die Begriffsdefinition „Befehlsnachricht“ wurde aus 03-02-01-W-101 „Betriebserprobung Digitaler Befehl“ übernommen und redaktionell aktualisiert.

DB InfraGO

Beabsichtigte Änderungen
Digitaler Befehl - Anforderungen an Tf-Endgeräte
synoptische Darstellung Version 1.7 zu Version 2.0

Änderungsart: NEU · GEÄNDERT · ZUSAMMENGEFÜHRT · UMGESTUFT · UNVERÄNDERT · ENTFALLEN

Hinweis: V2.0 ist entlang der DIN EN ISO/IEC 27002:2024-01 neu strukturiert; V2.0-Fundstelle jeweils in Klammern (Kapitel · ISO-Control). „—" = neue Anforderung ohne Vorgänger in V1.7. Die Regelungen sind als sinngemäße Zusammenfassung zur Orientierung formuliert. Verbindlich ist ausschließlich der Wortlaut der jeweils gültigen Fassung (V1.7 bzw. V2.0).

Abschnitt / Punkt	Regelung alt (V1.7)	Regelung neu (V2.0)	Änderungsgrund / Anmerkungen
1 Grundlagen und Struktur			
Aufbau & normative Grundlage GEÄNDERT	Gliederung in „Anforderungen an das Endgerät", „Anforderungen an die eingesetzte Software" und „Organisatorische Anforderungen"; keine Zuordnung zu einem Sicherheitsstandard.	Kapitel 2 gliedert die Sicherheitsanforderungen in organisatorische, physische und technische Anforderungen. Kapitel 3 enthält verpflichtende und empfohlene System- und Konnektivitätsanforderungen. Die Sicherheitsanforderungen sind geeigneten Controls der DIN EN ISO/IEC 27002:2024-01 zugeordnet und berücksichtigen die „Bedrohungsanalyse Digitaler Befehl" vom 04.08.2025.	Grundlegende Neustrukturierung; Sicherheitsanforderungen werden von System- und Konnektivitätsanforderungen getrennt und normativ sowie risikobasiert hergeleitet.
Geltungsbereich GEÄNDERT	Notebooks, Smartphones und Tablets unter Windows, Linux, Android und iOS.	Als mobile Endgeräte gelten Notebooks, Smartphones und Tablets. Die herstellerunspezifischen Anforderungen sind für Windows-, Linux-, Android- und iOS-Plattformen umzusetzen und gelten gleichermaßen für Ersatz- und Austauschgeräte.	Der grundsätzliche Geltungsbereich bleibt bestehen. Ersatz- und Austauschgeräte werden nun ausdrücklich einbezogen.
2.1 Organisatorische Anforderungen			
Lifecycle – Beschaffung und Inventarisierung GEÄNDERT	Smartphones und Tablets müssen aus aktuellen Modellreihen stammen. End-of-Life und End-of-Service sind zu beachten; die Versorgung mit Sicherheitsupdates ist sicherzustellen.	Endgeräte müssen aus aktuellen Modellreihen bezogen und inventarisiert werden. Herstellerangaben zu End-of-Life und End-of-Service sind zu beachten. Sicherheitsupdates für Firmware, Betriebssysteme und Anwendungen sind nach ihrer Bereitstellung im Rahmen eines risikobasierten Patch- und Schwachstellenmanagements nach dem Stand der Technik fristgerecht zu installieren. → ISO 5.9, 5.19	Auf alle Endgerätetypen erweitert; Inventarisierung, Firmware und Anwendungen ausdrücklich aufgenommen. Starre Aktualisierungsvorgaben werden durch ein risikobasiertes Verfahren ersetzt.
Lifecycle - Verwundbare Komponenten GEÄNDERT	Hardwarekomponenten mit bekannten Schwachstellen dürfen nicht eingesetzt werden. Die Überwachung liegt bei den endgeräteausgebenden Unternehmen.	Hardware- und Softwarekomponenten dürfen nicht eingesetzt werden, wenn für eine bekannte, noch nicht behobene Schwachstelle öffentlich verfügbarer Exploit-Code oder ein Proof of Concept vorliegt und die Risikobewertung ergibt, dass die Sicherheit des Verfahrens mehr als nur unerheblich beeinträchtigt werden kann. In diesen Fällen ist unverzüglich über Sicherheitsupdates, wirksame Kompensationsmaßnahmen oder die Sperrung der betroffenen Komponenten zu entscheiden. → ISO 5.19	Softwarekomponenten werden einbezogen. Das pauschale Verbot wird durch konkrete Risiko- und Entscheidungskriterien sowie verbindliche Reaktionsmöglichkeiten ersetzt.
Ordnung - Benutzungsordnung NEU	Keine übergreifende Benutzungsordnung; einzelne Vorgaben bestanden insbesondere zu Passwörtern und Berechtigungen.	Für die Endgerätenutzung muss eine verbindliche, rollenbasierte Benutzungsordnung gelten. Sie muss den zulässigen Umgang mit Geräten und Daten regeln, die Einhaltung der Anforderungen sicherstellen und Berechtigungen auf das benötigte Mindestmaß beschränken. → ISO 5.10, 5.15	Neue übergreifende organisatorische Regelung. Technisch umsetzbare Schutzmaßnahmen werden dadurch nicht ersetzt.
Ordnung / Rückgabeprozess NEU	Keine entsprechende Regelung.	Nicht mehr genutzte oder benötigte Endgeräte müssen im Rahmen eines geregelten Rückgabeprozesses wieder eingesammelt werden. → ISO 5.11	Rückgabe und Aussonderung werden erstmals verbindlich geregelt.

Abschnitt / Punkt	Regelung alt (V1.7)	Regelung neu (V2.0)	Änderungsgrund / Anmerkungen
2.2 Physische Anforderungen			
Hardware NEU	Keine entsprechende Regelung.	Endgeräte müssen entsprechend ihrem Einsatzzweck und Einsatzort stabil und zuverlässig ausgewählt und gegen Beschädigung geschützt werden. Defekte Geräte dürfen nicht eingesetzt werden, wenn Hardwaredefekte Ablese-, Eingabe- oder Bestätigungsfehler verursachen können. → ISO 7.5, 7.13	Physische Geräteeignung und der Umgang mit sicherheitsrelevanten Hardwaredefekten werden erstmals geregelt.
Anzeige GEÄNDERT	System- oder anwendungsspezifische Elemente dürfen die vollständige und dauerhafte Sichtbarkeit des Digitalen Befehls nicht beeinträchtigen.	System- oder anwendungsspezifische Elemente dürfen die vollständige und dauerhafte Sichtbarkeit oder Funktionsfähigkeit des Digitalen Befehls nicht beeinträchtigen. → ISO 7.7 f)	Schutzumfang um die Funktionsfähigkeit erweitert; die Mindestbildschirmgröße wird getrennt in Kapitel 3.1 geregelt.
Aufbewahrung NEU	Keine entsprechende Regelung.	Nicht genutzte Endgeräte sind so zu behandeln und aufzubewahren, dass sie vor unbefugtem Zugriff und unbemerkter Manipulation geschützt sind. → ISO 7.9	Physischer Schutz nicht genutzter Endgeräte wird neu aufgenommen.
2.3 Technische Anforderungen			
Verschlüsselung ZUSAMMENGEFÜHRT	Drei Anforderungen: vollständige Verschlüsselung des internen Speichers; gleichwertige Verschlüsselung von Wechseldatenträgern; Verwendung aktueller und sicherer Verschlüsselungsalgorithmen beziehungsweise -techniken. Die Verschlüsselung muss auf Nutzerkennwort und Gerätemerkmalen beruhen.	Integrierte Speicher und Wechselspeicher müssen verschlüsselt sein. Die Verschlüsselung muss auf einem Nutzergeheimnis und gerätespezifischen Merkmalen, beispielsweise einem Trusted Platform Module, basieren. Zulässig sind nur nach BSI TR-02102 als sicher geltende Verfahren. → ISO 8.1 h), n)	Die bisherigen Einzelanforderungen werden zusammengeführt. Zweck, technische Grundlage und zulässiger Sicherheitsstandard werden konkretisiert.
Diebstahl NEU	Keine entsprechende Regelung.	Bei Verlust oder Diebstahl muss eine entfernte Außerbetriebnahme des Endgeräts durch Verriegelung, Löschen oder Vernichten von Schlüsselmaterial möglich sein. → ISO 8.1 j)	Technische Reaktion auf Verlust und Diebstahl wird erstmals gefordert.
Authentifizierung GEÄNDERT	Mindestens ein Entsperrmechanismus aus einer festen Liste: alphanumerisches Passwort, Fingerabdruck, Gesichtserkennung oder Hochsicherheits-Biometrie. Passwortanforderungen waren separat geregelt.	Das Endgerät muss über mindestens einen nach dem Stand der Technik sicheren Entsperrmechanismus verfügen, beispielsweise ein alphanumerisches Passwort oder Biometrie. Geheimnisse müssen einzigartig, nicht erratbar und geheim sein; ihre Qualität ist zu prüfen und technisch sicherzustellen. → ISO 5.17, 8.5	Die feste Verfahrensliste wird durch eine technologieoffene Anforderung ersetzt; Anforderungen an Authentisierungsgeheimnisse werden integriert.
Malware – Schutz gegen Schadsoftware GEÄNDERT	Virenschutz auf allen Endgeräten; Ausnahmen waren zu begründen. Virendefinitionen mussten mindestens täglich aktualisiert werden. Der Schutz durfte durch Nutzer nicht deaktiviert werden. Zusätzlich waren ein Virenschutzkonzept und Benutzerschulungen gefordert.	Alle Endgeräte müssen über einen täglich aktualisierten Schutz gegen Schadsoftware verfügen, beispielsweise Virenscanner oder Allowlisting. Meldungen sind durch Fachpersonal zu analysieren und erforderlichenfalls zu beheben. Der Schutz sollte auch Software erkennen, die durch Einblendungen die Ablesbarkeit beeinträchtigen kann. → ISO 8.7	Der Begriff „Virenschutz“ wird technologieneutral erweitert. Die Auswertung durch Fachpersonal ist neu; Nicht-Deaktivierbarkeit, Virenschutzkonzept und Benutzerschulung werden nicht ausdrücklich übernommen.
Malware – Webfilterung	Keine entsprechende Regelung.	Endgeräte müssen über einen Webfilter gegen schädliche und betrügerische Inhalte verfügen. Der Webfilter kann Bestandteil des Schutzes	Zusätzlicher Schutz vor schädlichen beziehungsweise betrügerischen

Abschnitt / Punkt	Regelung alt (V1.7)	Regelung neu (V2.0)	Änderungsgrund / Anmerkungen
NEU		gegen Schadsoftware sein. → ISO 8.23	Webinhalten.
Betriebssystem GEÄNDERT	Anwendungen und Browser mussten aktuell gehalten werden. Neue Versionen waren innerhalb von vier Wochen, Sicherheitsupdates innerhalb einer Woche zu installieren. Betriebssysteme mussten regelmäßig aktualisiert werden; nicht mehr unterstützte Betriebssysteme durften nicht eingesetzt werden.	Betriebssysteme und Anwendungen müssen aktuell sein und vom Hersteller aktiv mit Fehlerbehebungen versorgt werden. Schwachstellen sind im Rahmen eines risikobasierten Patch- und Schwachstellenmanagements fristgerecht nach dem Stand der Technik zu behandeln. Endgeräte mit nicht mehr sicherheitsgepflegter Software dürfen nicht eingesetzt werden. Die Verantwortung liegt bei den endgeräteausgebenden Unternehmen. → ISO 8.8, 8.19	Der Anwendungsbereich wird erweitert und risikobasiert formuliert. Die festen Fristen von einer beziehungsweise vier Wochen entfallen.
Browser GEÄNDERT	Zugelassen waren Google Chrome und Microsoft Edge. Bei gravierenden Schwachstellen musste bis zur Behebung auf den anderen freigegebenen Browser ausgewichen werden. Darstellungs- oder verhaltensbeeinflussende Plugins waren unzulässig.	Es dürfen ausschließlich die in Kapitel 3.1 freigegebenen Browser eingesetzt werden. Plugins, die Darstellung oder Verhalten des Digitalen Befehls beeinflussen, sind unzulässig. → ISO 8.8	Die Browserliste wird nach Kapitel 3.1 verlagert. Die ausdrückliche Ausweichregel bei gravierenden Browser-Schwachstellen entfällt.
Härtung GEÄNDERT	Das Betriebssystem von Notebooks musste durch Sicherheitseinstellungen, Benutzereinschränkungen und Virenschutz abgesichert werden. Standard-Benutzer und Standard-Gruppen waren zu löschen oder zu deaktivieren.	Betriebssystem und Anwendungen müssen einsatzzweckgerecht abgesichert werden. Eine Härtung nach CIS-Benchmarks wird empfohlen. Nicht benötigte Anwendungen, Benutzer, Zugänge und rückwärtskompatible Authentisierungsverfahren sind zu entfernen. → ISO 8.9	Härtung gilt für alle Endgeräte sowie für Betriebssystem und Anwendungen. Nicht benötigte Konfigurationen werden umfassender erfasst.
Datenschutz GEÄNDERT	Herstellertelemetrie musste deaktiviert oder auf ein Minimum begrenzt werden. Daten aus Anwendungen durften nicht übermittelt werden.	Telemetrie- und Diagnosedaten des Endgeräts sowie der eingesetzten Anwendungen sind auf das zwingend erforderliche und technisch beeinflussbare Minimum zu beschränken. Fachliche Inhaltsdaten und sicherheitsrelevante Verfahrensdaten des Digitalen Befehls dürfen nicht an Hersteller oder Dritte übertragen werden, soweit dies durch Plattform- oder Anwendungseinstellungen technisch beherrschbar ist. → ISO 8.12	Der Anwendungsbereich wird auf Diagnose- und Anwendungsdaten erweitert. Das Übermittlungsverbot umfasst neben Herstellern auch sonstige Dritte und wird technisch abgrenzbar formuliert.
Rechte GEÄNDERT	Einrichtung, Betriebssystem- und App-Installation mussten zentral erfolgen. Nutzer durften keine Betriebssysteme installieren, sicherheitsrelevante Konfigurationen ändern oder Apps aus anderen als zentral bereitgestellten Quellen installieren. Administrator- und Root-Rechte waren zusätzlich ausdrücklich verboten.	Einrichtung der Endgeräte sowie Installation von Betriebssystem und Apps müssen verwaltet erfolgen. Nutzer dürfen keine Betriebssysteme installieren, sicherheitsrelevante Konfigurationen verändern oder nicht freigegebene Anwendungen installieren. → ISO 8.18	„Zentral“ wird durch „verwaltet“ ersetzt; sicherheitsrelevante Konfigurationen werden beispielhaft konkretisiert. Ein ausdrückliches Verbot von Administrator- oder Root-Rechten ist nicht mehr enthalten.
Netzwerk NEU	Keine entsprechende Regelung.	Die Netzwerkschnittstellen der Endgeräte müssen gegen Angriffe geschützt sein. Ein- und ausgehende Verbindungen sind durch eine Firewall auf das für die Nutzung erforderliche Mindestmaß zu beschränken. Dies gilt insbesondere für Dienste mit hohen Bandbreitenanforderungen, die die verzögerungsfreie Durchführung des Digitalen Befehls beeinträchtigen könnten. → ISO 8.20, 8.21	Neue technische Anforderung an Netzwerksicherheit, Verbindungsbeschränkung und Schutz der für das Verfahren benötigten Bandbreite.
3 System- und Konnektivitätsanforderungen			
3.1 Mindestbildschirmgröße UNVERÄNDERT	Mindestbildschirmgröße nach Skalierung von 360 px (dp).	Mindestbildschirmgröße nach Skalierung von 360 px (dp) als verpflichtende Systemanforderung.	Inhaltlich unverändert; aus der Darstellungsanforderung in die verpflichtenden Systemanforderungen

Abschnitt / Punkt	Regelung alt (V1.7)	Regelung neu (V2.0)	Änderungsgrund / Anmerkungen
			verschoben.
3.1 Freigegebene Browser UNVERÄNDERT	Freigegebene Browser: Google Chrome und Microsoft Edge.	Freigegebene Browser: ausschließlich Google Chrome und Microsoft Edge.	Inhaltlich unverändert; Browserliste wird als eigenständige verpflichtende Systemanforderung geführt.
3.2 Empfohlene Systemanforderungen für Smartphones und Tablets NEU	Keine entsprechende Regelung.	Das Endgerät sollte über mindestens 6 GB RAM verfügen.	Neue empfohlene Systemanforderung für Smartphones und Tablets.
3.3 Empfohlene Systemanforderungen für Laptops NEU	Keine entsprechende Regelung.	Das Endgerät sollte über mindestens 8 GB RAM verfügen.	Die bislang verpflichtenden Anforderungen werden zu Empfehlungen umgestuft; die Bandbreite muss nun dauerhaft für das Verfahren verfügbar sein.
3.4 Konnektivität und Bandbreite UMGESTUFT	Das Endgerät muss eine stabile Internetverbindung aufbauen können. Die Übertragungsgeschwindigkeit muss mindestens 1 Mbit/s betragen.	Die empfohlenen System- und Konnektivitätsanforderungen bilden die Grundlage für eine ordnungsgemäße und performante Nutzung. Für Performance-Einschränkungen infolge von Abweichungen übernimmt der Betreiber keine Verantwortung.	Verantwortungsabgrenzung für Abweichungen von den empfohlenen Anforderungen.
3.5 Abschließender Hinweis NEU	Keine entsprechende Regelung.	Die Einhaltung der empfohlenen System- und Konnektivitätsanforderungen aus den Abschnitten 3.2 bis 3.4 bildet die Grundlage für eine ordnungsgemäße und performante Nutzung des Digitalen Befehls. Abweichungen können zu Performance-Einschränkungen führen, für die der Betreiber des Digitalen Befehls keine Verantwortung übernimmt.	Neuer abschließender Hinweis zur Bedeutung der Empfehlungen und zur Verantwortungsabgrenzung bei Abweichungen.
4 Entfallene bzw. überführte Einzelvorgaben			
Passwortvorgaben ZUSAMMENGEFÜHRT	Sichere Passwörter waren vorzugeben; triviale Passwörter waren zu verbieten und geheim zu halten. Nicht technisch umsetzbare Vorgaben mussten organisatorisch angewiesen werden.	Geheimnisse müssen einzigartig, nicht erratbar und geheim sein. Ihre Qualität ist zu prüfen und technisch sicherzustellen; ergänzend gilt die Benutzungsordnung.	Redundanzabbau; Vorgaben in die neuen Kategorien integriert – kein inhaltlicher Wegfall.
Administrator- und Root-Rechte ENTFALLEN	Nutzer durften keine Administrator- oder Root-Berechtigungen erhalten.	Kein ausdrückliches Verbot. Die Benutzungsordnung fordert lediglich eine Beschränkung auf das benötigte Mindestmaß.	„Least Privilege“ ist kein gleichwertiger Ersatz für das bisherige ausdrückliche Verbot.
Verantwortung für das Schwachstellenmanagement ENTFALLEN	Die endgeräteausgebenden Unternehmen waren für Schwachstellenüberwachung und Updates verantwortlich. Nutzer mussten die entsprechenden Anweisungen befolgen.	Die Verantwortung der endgeräteausgebenden Unternehmen für Schwachstellenüberwachung und Sicherheitsupdates bleibt bestehen. Eine ausdrückliche Mitwirkungs- und Befolgungspflicht der Nutzer wird nicht mehr genannt.	Unternehmensverantwortung übernommen; ausdrückliche Nutzerpflicht entfällt.

Abschnitt / Punkt	Regelung alt (V1.7)	Regelung neu (V2.0)	Änderungsgrund / Anmerkungen
Nicht-Deaktivierbarkeit des Virenschutzes **ENTFALLEN**	Der Virenschutz durfte durch Nutzer nicht deaktiviert werden können.	Keine ausdrückliche Anforderung an die technische Nicht-Deaktivierbarkeit des Schutzes gegen Schadsoftware.	Die Vorgabe ist nicht gleichwertig in V2.0 enthalten.
Virenschutzkonzept und Benutzerschulung **ENTFALLEN**	Verantwortlichkeiten mussten in einem Virenschutzkonzept geregelt und Nutzer für den Fall eines Virenbefalls geschult werden.	Meldungen der Schutzsysteme müssen durch Fachpersonal analysiert und gegebenenfalls behoben werden. Ein Schutzkonzept und Benutzerschulungen werden nicht verlangt.	Fachliche Auswertung wird neu geregelt; Konzept- und Schulungspflichten entfallen.
Zugriff anderer Apps auf Verfahrensinformationen **ENTFALLEN**	Apps waren zentral zu verwalten; es war sicherzustellen, dass sie keinen Zugriff auf Informationen aus dem Digitalen Befehl erhalten.	Keine ausdrückliche Vorgabe zur Isolation der Verfahrensdaten gegenüber anderen Anwendungen.	Die bisherige Anforderung an App-Isolation beziehungsweise Zugriffstrennung wird nicht übernommen.

DB InfraGO

Beabsichtigte Änderungen
Digitaler Befehl – Geteilte Risiken
synoptische Darstellung

Abschnitt / Punkt	Regelung alt (Anlage Betriebserprobung Digitaler Befehl)			Regelung neu (Anlage Ril 408.2412)			Änderungsgrund / Anmerkungen
Geteilte Risiken - Probleme mit dem Endgerät des Tf	Probleme mit dem Endgerät des Tf	Probleme mit den Endgeräten der Tf sind durch das EVU zu betrachten (z. B. Ausfall des Endgerätes oder eine gestörte Anzeige, während ein gültiger Befehl vorliegt).	Es können Handlungsanweisungen für den Tf zur Verfügung gestellt werden, wie bei einem Ausfall des Endgerätes zu Verfahren ist. Alternativ können Rückfallebenen geschaffen werden. Der Fdl hat stets die Möglichkeit den Befehl im konventionellen Verfahren nach Ril 408.0411 zu übermitteln.	Probleme mit dem Endgerät des Tf	Probleme mit den Endgeräten der Tf sind durch das EVU zu betrachten (z. B. Ausfall des Endgerätes oder eine gestörte Anzeige, während ein gültiger Befehl vorliegt).	Ril 408.2412 2.3 „Rückfallebene Digitaler Befehl" gibt bereits Handlungsanweisungen vor. Es können darüber hinaus Handlungsanweisungen für den Tf zur Verfügung gestellt werden, wie bei einem Ausfall des Endgerätes zu verfahren ist. Alternativ können Rückfallebenen geschaffen werden. Der Fdl hat stets die Möglichkeit den Befehl im konventionellen Verfahren nach Ril 408.0411 zu übermitteln.	Da in Ril 408.2412 2.3 bereits Regelungen für die Rückfallebene Digitaler Befehl vorgegeben sind wurden diese hier aufgegriffen und präzisiert, dass darüberhinausgehende Handlungsanweisungen getroffen werden können.