EUROPEAN UNION AGENCY FOR RAILWAYS

Jak zlepšit fungování železniční soustavy pro společnost.

Příručka

Příručka dohledu

	Vyhotovil	*Ověřil*	*Schválil*
Jméno	S. D'ALBERTANSON	M. SCHITTEKATTE	C. CARR
Funkce	vedoucí odpovědný za projekt	projektový manažer	vedoucí oddělení
Datum	29/06/2018	29/06/2018	29/06/2018
Podpis			

Historie dokumentu

Verze	*Datum*	*Poznámky*
1.0	29/06/2018	Konečná verze k zveřejnění

Tento dokument není právně závazným předpisem Evropské agentury pro železnice. Nejsou jím dotčeny rozhodovací procesy stanovené příslušnými právními předpisy EU. Závazný výklad právních předpisů EU je výlučně v kompetenci Soudního dvora Evropské unie.

1. Úvod

1.1 Účel příručky

Vnitrostátní bezpečnostní orgány *(National Safety Authority*, NSA) v Evropě se liší svou velikostí a komplexností. Tato příručka stanoví, jak mohou orgány NSA vykonávat dohled primárně nad svými provozovateli infrastruktury a železničními podniky, ale případně také nad subjekty odpovědnými za údržbu, a to jednotným způsobem odpovídajícím jejich velikosti. Příručka si klade za cíl vysvětlit orgánům NSA a jiným zainteresovaným subjektům úlohu, kterou hraje dohled v evropské železniční soustavě, a jak souvisí s hodnocením bezpečnosti.

Poznámka; za účelem dohledu nad přepravou nebezpečných nákladů po železnici může vnitrostátní bezpečnostní orgán zastávat roli způsobilé authority, nebo zastávat roli koordinační, v případě potřeby spolupracující s jakýmkoli jiným příslušným orgánem.

1.2 Co je dohled?

Dohled znamená režim zavedený vnitrostátním bezpečnostním orgánem za účelem dohledu nad účinností systému zajišťování bezpečnosti poté, co udělil osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti a dohledu nad trvalým dodržováním všech nezbytných požadavků.

Tento dohled se vztahuje na kroky orgánu NSA, které zajišťují, aby organizace, které bylo vydáno jednotné osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti, provozovala svůj systém řízení bezpečnosti tak, aby efektivně řídil riziko v průběhu platnosti tohoto osvědčení o bezpečnosti, a také na řadu dalších specifických činností definovaných v nařízení Komise v přenesené pravomoci (EU) 2018/761 (dále jen „společná bezpečnostní metoda pro dohled“). Za účelem výkonu dohledu by měl vnitrostátní bezpečnostní orgán zajistit, že má způsobilé osoby, které jsou vybrány a jejichž způsobilost je udržovány prostřednictvím systému řízení způsobilosti.

Společná bezpečnostní metoda (CSM) pro dohled provádí požadavky směrnice (EU) 2016/798, které se týkají povinnosti orgánů NSA provádět dohled nad železničními podniky a provozovateli infrastruktury v jejich jurisdikci po vydání jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti.

Článek 17 směrnice 2016/798 ukládá, aby orgány NSA dohlížely na průběžné plnění zákonné povinnosti uložené článkem 9 směrnice železničním podnikům a provozovatelům infrastruktury, vyžadující používání systému řízení bezpečnosti (SMS). Při výkonu této funkce musí orgány NSA zajistit, aby jejich dohledové aktivity obsahovaly mj.:

- *monitorování účinnosti využívání celého systému SMS nebo jeho části železničními podniky nebo provozovateli infrastruktury;*
- *monitorování správného využívání relevantních společných bezpečnostních metod (CSM) železničními podniky nebo provozovateli infrastruktury prostřednictvím jejich systému SMS i v případě, kdy je železniční podnik nebo provozovatel infrastruktury subjektem odpovědným za údržbu svých vozidel, který nemá osvědčení v souladu s nařízením o subjektech odpovědných za údržbu;*
- *monitorování, zda prvky interoperability na jeho území vyhovují základním požadavkům uloženým článkem 8 směrnice (EU) 2016/797 prostřednictvím systému SMS železničního podniku nebo provozovatele infrastruktury.*

V návaznosti na výsledky dohledu mohou orgány NSA přijmout odpovídající donucovací opatření (např. dočasná bezpečnostní opatření), která mají dosáhnout shody s právními předpisy, odhalit příležitosti ke

zlepšení vnitrostátních právních předpisů za účelem zvýšení efektivity a informovat zainteresované subjekty o změnách bezpečnostního regulačního rámce a nových rizicích nebo zvýšení rizik v jejich členských státech.

Dohled se obvykle provádí v jazyce členského státu, v němž dohled probíhá, není-li uzavřena dohoda mezi příslušným orgánem NSA pro danou oblast provozu a organizací, v níž probíhá dohled, o tom, že se použije jiný jazyk.

1.3 Komu je určena tato příručka?

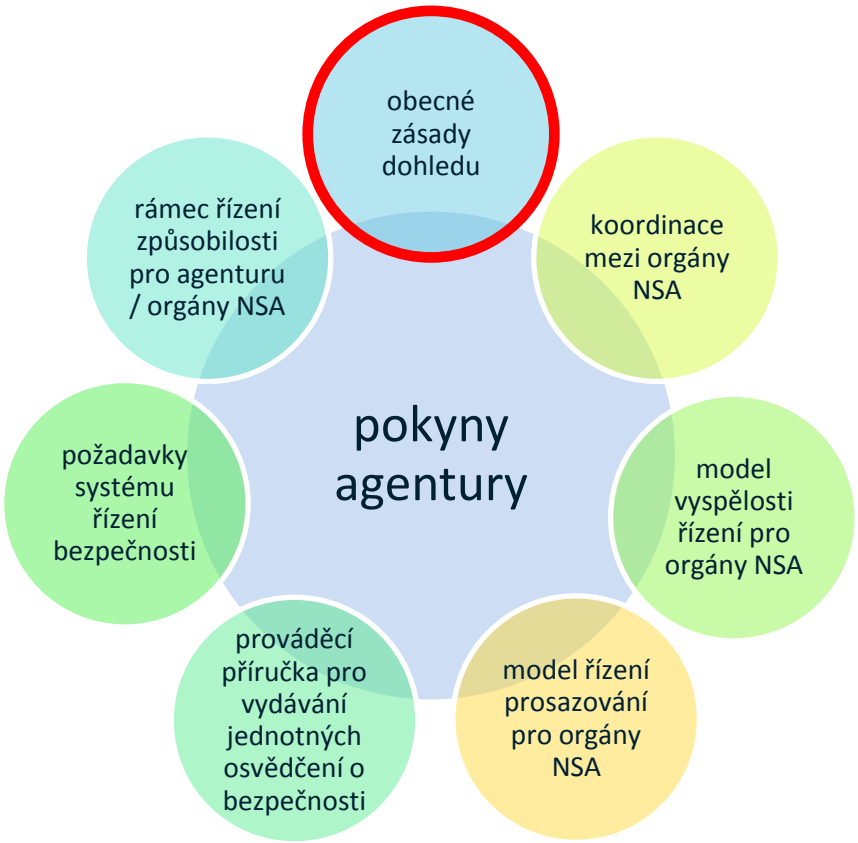
Tato příručka je určena v první řadě orgánům NSA a pomáhá jim plnit požadavky společné bezpečnostní metody pro dohled po vydání jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti. Příručka je rovněž k dispozici subjektům, které jsou předmětem dohledu, umožňuje jim dozvědět se, co mohou očekávat v průběhu jejich vztahu s orgánem NSA, a pomáhá jim tak adekvátně plánovat a organizovat.

1.4 Působnost

V příručce jsou uvedeny podrobné praktické informace umožňující lépe porozumět požadavkům kladeným na dohled, které jsou stanoveny v právním rámci EU.

1.5 Struktura pokynů

Tento dokument tvoří součást souboru pokynů agentury, které mají pomoci železničním podnikům, provozovatelům infrastruktury, vnitrostátním bezpečnostním orgánům a agentuře při výkonu jejich funkce a provádění prací v souladu se směrnicí (EU) 2016/798.



Obr. 1: Soubor pokynů agentury

1.6 Kdo je předmětem dohledu?

Z právního rámce popsaného výše je zřejmé, že orgány NSA musí dohlížet na ty subjekty, které mají jednotné osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti, tedy na železniční podnik, resp. provozovatele infrastruktury. Provádí dohled za tím účelem, aby ověřily, zda tyto subjekty plní svůj závazek provozovat systém SMS, který řídí riziko, uvedený v žádosti o jednotné osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti.

Obsah

2. Definice

V této příručce se používají tyto definice:

Relevantní zainteresované osoby

Relevantními zainteresovanými osobami se označují osoby, které hrají určitou úlohu při provozu železnice nebo které jsou jím dotčeny a jsou zainteresovány na bezpečnostních výstupech, např. odvětvové orgány, organizace cestujících nebo místní orgány.

Zbytečná zátěž

Tento výraz znamená, že pokud má být u železničního podniku proveden dohled, koordinují se práce tak, aby v železničním podniku neprobíhaly dva různé dohledy, které vyžadují současné dotazování týchž osob, nebo aby u něj v rámci dohledu ve stejných termínech neprobíhalo více návštěv různých osob z téhož odboru. Jedná se o co nejefektivnější plánování nezbytných zásahů, které umožňují vykonávat práci v rozumných termínech, aniž by v organizaci, kde probíhá dohled, docházelo k většímu narušení provozu.

Řídicí mechanismy

Řídicími mechanismy se označují procesy a procedury systému SMS uplatňované železničním podnikem nebo provozovatelem infrastruktury, kterými se řídí bezpečnost a plní jeho bezpečnostní cíle za současného dodržování jeho zákonných povinností a dalších požadavků relevantních pro bezpečnost.

Závažné porušení předpisů

Závažným nesouladem je takový problém zjištěný vnitrostátním bezpečnostním orgánem, jehož odchylka od očekávaného stavu je taková, že musí být přijata nápravná opatření pod vedením daného vnitrostátního bezpečnostního orgánu nebo v případě záležitostí, které jsou postoupeny orgánu udělujícímu osvědčení, přičemž je třeba vzít v úvahu možnost odnětí nebo omezení jednotného osvědčení o bezpečnosti nebo schválení za účelem zajištění bezpečnosti.

Jakékoli jiné problematické oblasti

Jakékoli další problematické oblasti se vztahují k situaci, kdy vnitrostátní bezpečnostní orgán během dohledu zjistí odchylku od očekávaného stavu, ta však není natolik závažná, aby bylo potřebné přijmout okamžitou nápravu, ale je natolik závažná, aby vnitrostátní bezpečnostní orgán zaznamenal svá zjištění a informovala organizaci, nad níž je vykonáván dohled, o potřebě zlepšit situaci.

3. Dohled na základě rizik

Je možné nalézt určité důležité oblasti, které umožňují efektivní fungování dohledu na základě rizik. Jedná se o tyto oblasti:

- *orgán NSA musí v obecné rovině znát rizika v národní železniční soustavě a vědět, která z těchto rizik jsou nejzásadnější;*
- *orgán NSA musí dobře chápat manažerskou schopnost železničních podniků a provozovatelů infrastruktury (a souvisejících aktérů) řídit riziko;*
- *orgán NSA musí mít zaměstnance, kteří jsou způsobilí činit rozhodnutí ve všech bodech uvedených výše a dokáží dostatečně flexibilně upravovat svůj přístup, zpozorují-li růst či pokles rizik (viz Pokyny agentury k rámci řízení způsobilosti);*
- *orgán NSA musí čerpat informace pokud možno z co nejširšího spektra zdrojů (z železničního odvětví i mimo něj), které pomáhají při rozhodování o dohledu na základě rizik;*
- *orgán NSA musí umět odůvodnit svá rozhodnutí o tom, kde dohled provádět a kde nikoli;*
- *orgán NSA musí akceptovat také jiné důvody dohledu v členském státě, např. politické motivy nebo společenské ohledy, které nemusí vycházet z rizik;*
- *dohled se musí vázat k jednotnému osvědčení o bezpečnosti a schválení z hlediska bezpečnosti tak, aby se více zaměřoval na provozovatele nebo aktivity v provozu považované za rizikovější ihned po vydání jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti;*
- *vykonávaný dohled musí umožňovat orgánu NSA přesvědčit se, zda lze systémem SMS železničního podniku nebo provozovatele infrastruktury řídit rizika, která mu hrozí.*

Při provádění výše uvedených zásad by vnitrostátní bezpečnostní orgány měly mít určité prostředky (kvantitativní, semikvantitativní nebo kvalitativní) k pochopení rizika na úrovni státu. To má zásadní význam pro vypracování strategie dohledu. Bez jasné představy o rizicích, jimž je třeba čelit, není možné činit přiměřená a cílená rozhodnutí o tom, co a jakým nejlepším způsobem je třeba kontrolovat. Nedostatečné pochopení rizik v systému rovněž znamená, že při rozhovorech mezi státem a vnitrostátním bezpečnostním orgánem je promarněná příležitost se přiměřeně zamyslet nad tím, jak lze v rámci dostupných finančních prostředků zajistit zvýšení bezpečnost. Schopnost vnitrostátních dozorových orgánů objasnit členskému státu, jakými prostředky dosáhnout zvýšení bezpečnosti může být užitečným příspěvkem k vytváření příležitostí pro zlepšení bezpečnosti. Globální chápání bezpečnostních rizik v rámci systému je výchozím bodem ke zvýšenní bezpečnost.

Zde je také důležité uvést, že chápání obecného rizika v členském státě ze strany orgánu NSA by se nemělo výrazně lišit od chápání rizika vnitrostátního provozovatele infrastruktury. Lze například očekávat podobný názor na míru celkového rizika přejezdů v členském státě u provozovatele infrastruktury i orgánu NSA. Je-li názor provozovatele infrastruktury a NSA velmi odlišný, může ukazovat na selhání v systému řízení rizika.

Z hlediska způsobu dosažení všeobecného názoru na riziko v členském státě by na evropské úrovni bylo prospěšné, kdyby existovala konvergence ke standardní metodě provádění této práce. V této fázi však i mezi těmi zeměmi, které využívají podobné postupy, existují detailní rozdíly, které srovnání na evropské úrovni ztěžují. Současné postupy sahají od vysoce sofistikovaných až k velmi jednoduchým a tato skutečnost by mohla být odrazem vyspělosti železniční soustavy členského státu využívajícího evropský postup, jeho velikosti a také různých kulturních vlivů.

Hodnocení schopnosti jednotlivých aktérů v železniční soustavě řídit rizika vyžaduje schopnost orgánu NSA využívat dohled za účelem rozhodnout, jak efektivní jsou systémy řízení bezpečnosti organizací, nad nimiž

vykonává dohled. Pro většinu orgánů NSA se v praxi jedná o využívání vyškolených a způsobilých inspektorů, kteří umí tato rozhodnutí činit.

Vnitrostátní bezpečnostní orgány musí mít možnost využívat informace z co největšího počtu zdrojů, aby byly schopny křížové kontroly informací a aby se vyhnuly použití jediného souboru údajů ke stanovení priorit v oblasti dohledu. Vnitrostátní bezpečnostní orgány jsou rovněž nabádány, aby v případě potřeby využívaly informace o řízení rizik, a to i mimo odvětví železniční dopravy, za účelem ověření nálezů a k dalším zlepšení v procesech řízení rizik. Kromě údajů a zdrojů informací, které mají specifický význam, jako jsou údaje o nehodách nebo incidentech, lze využít deníky společností a výstupy modelů rizika v rámci členského státu, pokud jsou k dispozici. Za užitečné by však měly být považovány i jiné informace ze stížností nebo problémy vyplývající z vnímání veřejnosti nebo z akademických studií, na základě kterých je možné vypracování strategie a plánu pro dohled nad riziky.

V souladu s článkem 7 CSM pro dohled musí mít orgány NSA příslušná kritéria pro to, kdo bude předmětem dohledu a proč. Tato kritéria souvisí s plněním strategie. Účelem kritérií je dosáhnout toho, aby existoval jednotný postup uplatňovaný napříč dohledovými aktivitami a aby různí aktéři v systému dobře rozuměli tomu, proč jsou hodnoceny dané aktivity a jaká jsou měřítka úspěšnosti, podle nichž jsou posuzováni.

TSI OPE rovněž vyžaduje, aby vnitrostátní bezpečnostní orgány, v rámci své strategie a plánu dohledu, monitorovaly účinné dodržování pravidel (protože TSI OPE se zabývá procesem a pravidly, které přispívají k bezpečné operaci vlaku) v jejich každodenním poskytování dohledu nad SMS organizací, které regulují. Pokyny, které agentura zveřejnila ohledně používání základních zásad fungování stanovených v TSI OPE, budou vnitrostátním bezpečnostním orgánům pomáhat při provádění dohledu v této oblasti.

Orgány NSA mohou být rovněž pod tlakem z vnějších zdrojů, který nevychází z rizik. Může pocházet z obav veřejnosti z určitého aspektu železničního provozu, který se stane politickým důvodem k řešení této záležitosti. Tato skutečnost může, ale nemusí souviset s dohledovou strategií a dohledovým plánem, ale musí být zapracována do obou. Tyto záležitosti mohou mít velký pozitivní vliv na bezpečnost. Členský stát se tak může například rozhodnout odstranit do 10 let na svém území všechny přejezdy, zatímco přístup založený na riziku nemusí mít za cíl odstranit všechny přejezdy, nýbrž opatřit tyto přejezdy moderními zabezpečovacími systémy. Je zřejmé, že pokud se do 10 let přejezdy zcela odstraní, znamená to pro členský stát výrazný bezpečnostní přínos. Orgán NSA může být naopak vystaven tlaku plynoucímu z výhodnosti zachování přejezdů tam, kdy by podle přístupu založeného na riziku byly odstraněny.

Je důležité, aby dohled založený na riziku zohledňoval výsledky posouzení osvědčení o bezpečnosti a povolení k provozu. Je tomu tak proto, že posouzení osvědčení se ve většině případů bude zabývat uplatňováním systému zajišťování bezpečnosti v činnostech železničního podniku nebo provozovatele infrastruktury pouze na papíře. Otázka, zda aplikace funguje v praxi, je předmětem dohledu. Pro stávající železniční podniky a provozovatele infrastruktury, kteří mají dlouhou historii v rámci odvětvového dohledu, může být dohled rovnoměrně rozložený na celou dobu platnosti osvědčení. Pro nové účastníky systému může být vhodné zvýšit dohled na začátku doby životnosti certifikátu nebo po zahájení provozu na se zaměřením na konkrétní prvky systému řízení bezpečnosti, aby bylo zajištěno, že to, co je napsáno na papíře, je skutečně uvedeno do praxe soudržným způsobem. Pro stávající společnosti i nové účastníky je nezbytné, aby rozsah činností dohledu byl cílený a to na základě rizika.

Protože zdroje v orgánech NSA k provádění dohledu bývají omezené, je při rozhodování o tom, nad čím vykonávat dohled na základě rizik a proč, podstatné to, aby byla řešena otázka, kde dohled přinese nejvyšší hodnotu. Může se například stát, že provozovatel infrastruktury ví o problémech s prasklými kolejnicemi, a má program, kterým toto riziko řídí. Musí-li orgán NSA na této záležitosti trávit mnoho času, nemusí se jednat o optimální využití jeho zdroje. Orgán NSA se může místo toho rozhodnout, že se zaměří na oblast, kde se má za to, že provozovatel infrastruktury spíše nedokáže problém řešit.

4. Dohledová strategie

Článek 3 CSM pro dohled ukládá, aby orgány NSA měly dohledovou strategii, která obsahuje prvky uvedené v příloze I CSM. Navrhovaný vzor dohledové strategie je uveden v Příloha k této příručce. Nadpisy ve vzoru jsou určeny k tomu, aby umožnily jednotný postup při vytváření dohledových strategií napříč členskými státy a budovaly důvěru mezi orgány NSA, že jsou dodržovány bezpečnostní úrovně. Protože agentura hraje určitou úlohu při sledování činnosti orgánu NSA, pomohla by při výkonu této funkce společná struktura těchto strategií.

4.1 Výchozí stav

Při popisování výchozího stavu postačuje základní údaj o velikosti železniční sítě v členském státě a počtu železničních podniků a provozovatelů infrastruktury. V tomto oddílu je také nutné uvést dobu, po kterou je aplikována dohledová strategie, a mechanismy její kontroly.

4.2 Cíl

V cíli nebo záměru musí být uveden účel strategie, např. „spolupracovat s celým odvětvím za účelem průběžně zlepšovat výsledky v oblasti řízení bezpečnosti“. V oddílu musí být rovněž uvedena informace o tom, jak bude tento cíl splněn.

4.3 Zásady dohledu

Zásady jsou zopakováním závazku vnitrostátního bezpečnostního orgánu (VBO) vůči klíčovým hodnotám, které zajišťují, že rozhodování při výkonu dohledu je přísné, ale spravedlivé. Příloha společné metody (CSM) pro dohled se uvádí, že NSA při stanovování strategie dohledu a plánu (plánů), které z ní vyplývají, shromažďuje a analyzuje údaje/informace z řady zdrojů. Zdroje zahrnují informace z posouzení systémů řízení bezpečnosti, výsledky předchozí činnosti dohledu, odborné posouzení inspektorů, příslušné informace z povolení vozidla, zprávy vnitrostátních vyšetřovacích orgánů, údaje o nehodách nebo mimořádných událostech, výroční zprávy o bezpečnosti železničních podniků nebo provozovatelů infrastruktury, zprávy subjektů odpovědných za údržbu, stížnosti členů veřejnosti a další relevantní zdroje. Obecně řečeno, vnitrostátní bezpečnostní orgán by měl v zásadě získávat relevantní informace z místa, kde se nachází, za účelem identifikace oblastí rizika v rámci železničního systému členského státu. VBO bude muset posoudit a analyzovat dostupné informace, aby určil, které otázky jsou nejvýznamnější, a následně vypracovat strategii, která by se těmito otázkami zabývala společně s plánem, jehož cílem je zjistit, jak a v jakém období bude strategie realizována. Vnitrostátní bezpečnostní orgán musí pracovat na tom, jaké zdroje jsou zapotřebí k aplikaci navrhované strategie a plánu, a vyčlenit na jeho realizaci dostatečné zdroje. VBO se musí rovněž zabývat veškerými otázkami v rámci své strategie a plánu, které se týkají přeshraničních operací nebo infrastruktury, a podle potřeby koordinovat s jinými vnitrostátními bezpečnostními orgány.

Dohledové zásady, které má orgán NSA aplikovat, jsou odvozeny zejména z příloha CSM pro dohled. Orgán NSA musí provádět své dohledové aktivity postupem, který je v zásadě přísný a spravedlivý. Dosáhnout tohoto cíle pomáhají orgánům NSA zásady dohledu.

Vnitrostátní bezpečnostní orgány by měly uplatňovat zásadu **proporcionality** mezi prosazováním a rizikem. Opatření přijatá vnitrostátním bezpečnostním orgánem s cílem dosáhnout souladu nebo přivést železniční podniky a provozovatele infrastruktury k odpovědnosti za neplnění jejich právních povinností by měla být úměrná rizikům pro bezpečnost nebo potenciální závažnosti nesouladu, včetně jakékoli skutečné nebo

potenciální škody. Tato zásada je pro vnitrostátní bezpečnostní orgány zásadní, neboť přijetím tohoto přístupu prokazují těm které regulují, že uplatňují právo přiměřeným a spravedlivým způsobem. To snižuje potenciální obavy v regulovaných organizacích, že chyby nebo chyby budou muset mít za následek drakonický trest, což pak vytváří kulturu utajování a strachu, která nepodporuje robustní kontrolu rizik.

Vnitrostátní bezpečnostní orgány by měly uplatňovat zásadu **jednotnosti** přístupu s cílem zajistit, aby bezpečnostní orgán zaujal podobný přístup za podobných okolností k dosažení podobných cílů. Železniční podniky a provozovatelé infrastruktury chtějí, aby různí pracovníci, kteří vykonávají dohled v rámci jednoho vnitrostátního bezpečnostního orgánu, nebo v rámci různých vnitrostátních dozorových orgánů, pokud se jedná o přeshraniční opatření, s nimi zacházeli stejným způsobem. To jim dává jistotu a umožňuje jim lépe plánovat. Zabývá se rovněž otázkami týkajícími se kultury bezpečnosti a snižuje obavy ze strany železničních organizací nestátních subjektů.

Činnost dohledu vnitrostátního bezpečnostního orgánu by měla být **zaměřena** především na ty činnosti, u nichž je podle názoru vnitrostátního bezpečnostního orgánu zjištěno nejzávažnější riziko, nebo kde jsou rizika nejméně dobře kontrolována. Za tímto účelem by měl vnitrostátní bezpečnostní orgán disponovat metodami a nástroji pro posouzení výkonu řízení bezpečnosti železničních podniků a provozovatelů infrastruktury. V situaci, kdy jsou zdroje vzácné a požadavky na nestátní subjekty jsou četné, je nanejvýš důležité, aby se pozornost zaměřila na ta rizika, která jsou nejzávažnější. Tohoto je dosaženo analýzou výkonu řízení železničních podniků a provozovatelů infrastruktury ze strany vnitrostátních bezpečnostních orgánů.

Vnitrostátní bezpečnostní orgány by měly rozhodnout o svých prioritách tak, aby účinně využívaly své **zdroje**, avšak rozhodnutí o tom, jak nejlépe postupovat, by mělo být u každého jednotlivého vnitrostátního bezpečnostního orgánu. Činnosti by se měly zaměřit na ty, kteří nesou odpovědnost za riziko a kteří mají nejlepší předpoklady pro to, aby je mohli kontrolovat. Vnitrostátní bezpečnostní orgány mají omezené zdroje, takže je důležité, aby byly využívány rozumně, aby se maximalizovala účinnost vnitrostátního bezpečnostního orgánu v zaišťování toho, že odpovědné osoby řídí rizika odpovídajícím způsobem.

Vnitrostátní bezpečnostní orgány by měly uplatňovat zásadu **transparentnosti** s cílem pomoci železničním podnikům a provozovatelům infrastruktury pochopit, co se od nich očekává (včetně toho, co by měly nebo neměly dělat) a co by měli očekávat od vnitrostátního bezpečnostního orgánu. Pro železniční podniky a provozovatele infrastruktury je velmi důležité, aby pochopili, jak vnitrostátní bezpečnostní orgán rozhoduje, a tudíž chápaly, jaký bude pravděpodobný výsledek v případě, že nekontrolují riziko vhodným způsobem.

Vnitrostátní bezpečnostní orgány by měly být **zodpovědné** za svá rozhodnutí v souladu s čl. 18 odst. 3 směrnice (EU) 2016/798. Proto mají vnitrostátní bezpečnostní orgány vnitřní úpravu, podle níž mohou být vedeny k zodpovědnosti. Vnitrostátní bezpečnostní orgány by navíc měly mít také postup pro podávání stížností. Vnitrostátní bezpečnostní orgány činí rozhodnutí, z nichž některá budou mít nepříznivý dopad na ty železniční podniky a provozovatele infrastruktury, kteří neúčinně kontorolují rizika. Je důležité, aby vnitrostátní bezpečnostní orgány měly jasná kritéria pro přijímání těchto rozhodnutí tak, aby bylo jasné, jakým způsobem byly přijaty. Za druhé je velmi důležité, aby existoval postup pro napadení takových rozhodnutí, kdy se regulovaný subjekt domnívá, že vnitrostátní bezpečnostní orgán překročil své pravomoci nebo nepostupoval řádným způsobem.

Vnitrostátní bezpečnostní orgány by měly vypracovat dohody o **spolupráci** s jinými příslušnými orgány za účelem sdílení informací a vytvoření jednotných přístupů k otázkám, které mají dopad na bezpečnost železnic. Vnitrostátní bezpečnostní orgány musí mít zavedeny postupy pro sdílení příslušných informací mezi sebou a s dalšími příslušnými orgány. To má zásadní význam pro zajištění toho, aby správné opatření bylo v případě potřeby přijato správným orgánem.

Uplatňuje-li orgán NSA tyto zásady, zachází se s tím, u koho probíhá dohled, spravedlivě a v případě potřeby přísně. Je také dobré zmínit, že tyto zásady se vzájemně doplňují a společně prezentují orgán NSA subjektům,

které reguluje, jako příslušný a řádný orgán činící otevřeně a poctivě rozumné rozhodnutí. Připomínáme, že tyto zásady jsou znovu uvedeny v koncepci strategie dohledu, která je uvedena v příloze této příručky. Důvod spočívá v tom, že tato strategie je vysoce důležitá pro stanovení kritérií provádění dohledu, kdy orgán NSA reprodukováním zde uvedených zásad zdůrazňuje svůj závazek dodržovat tyto zásady a uvede důkazy, že postupuje transparentně.

Agentura rovněž vytvořila *příručku modelu řízení prosazování,* kterou mohou používat subjekty vykonávající dohled a která reflektuje výše uvedené zásady. Příručka bere zásady a aplikuje je na matici, jejímž účelem je sdělit pokyny pro osoby vykonávající dohled v tom smyslu, jak mají vypadat jejich rozhodnutí o prosazování na základě analýzy nedostatků v řízení rizik. Čím větší jsou nedostatky v řízení rizik, tj. rozdíl mezi očekávanou pozicí organizace, pokud by byla řádně uplatňována veškerá pravidla, a skutečnou pozicí, tím větší donucovací opatření lze očekávat.

4.4 Mechanismy dohledu

Opatření pro dohled by měla obecně zahrnovat strukturu řízení a personální zabezpečení vnitrostátního bezpečnostního orgánu (VBO), včetně vaby mezi osvědčením o bezpečnosti a schválením z hlediska bezpečnosti. Vnitrostátní bezpečnostní orgán by měl být transparentní, pokud jde o strukturu řízení, a o tom, jak jsou řešené otázky dohledu v případě potřeby eskalovány na vyšší úroveň a to včetně rozhodnutí o výkonávní rozhodnutí. Vnitrostátní bezpečnostní orgán by měl být rovněž transparentní, pokud jde o způsob, jakým přijímá rozhodnutí o regulaci rizik v jedné oblasti více než v jiném. VBO musí uvést, kdo jsou jeho zaměstnanci a obecně pak jakým způsobem zajišťuje jejich způsobilost (viz *Pokyny agentury k rámci řízení způsobilosti*) a na jakém základě své zaměstnance úkoluje. VBO by měl rovněž uvést, jak hodlá měřit výkonnost systémů řízení bezpečnosti jako součást svých činností v oblasti dohledu, například použitím modelů zralosti/modelů kultury bezpečnosti nebo jinými prostředky. Agentura vypracovala pokyny pro jeden navrhovaný model zralosti řízení, který může být použit jak bezpečnostními orgány, tak zúčastněnými stranami za tímto účelem. (viz též *pokyny agentury k modelu zralosti řízení*).

Jedna ze základních otázek pro orgány NSA spočívá v tom, jak jsou řízeni noví účastníci na trhu, neexistuje-li informace o dosavadní kvalitě jejich systému SMS. Některé orgány NSA z tohoto důvodu vydávaly prvním účastníkům na železničním trhu osvědčení o bezpečnosti na dobu kratší než 5 let. Některé orgány NSA se rozhodly provádět před vydáním osvědčení o bezpečnosti komplexnější audit nového účastníka nebo provádět tento audit ihned po vydání osvědčení. Omezená doba platnosti musí být odůvodněna tím, že je nezbytná k dosažení efektivního řízení rizik ovlivňujících bezpečnost železničního provozu. Orgány NSA mohou po vydání osvědčení provádět detailnější prověrku nových účastníků, která zajišťuje, aby jejich bezpečnostní mechanismy byly vhodné k danému účelu. NSA musí ve své dohledové strategii a plánech jednoznačně uvést, o jaké mechanismy se jedná.

4.5 Úrovně rizika v členském státě

V následujícím oddíle o úrovních rizika v členském státě musí být uvedeno, jak se k těmto úrovním rizika dospělo, např. použitím modelů rizika a/nebo vyspělosti, a související důvody, proč jsou ve strategii řešena některá rizika a jiná nikoli.

4.6 Strategické priority dohledu

V následujícím oddíle je nutné uvést, jak se stanoví strategické priority, které pojednávají o těchto bodech:

- *Jak se má provádět dohled nad systémy SMS. Zde orgán NSA uvede techniky dohledu (viz oddíl 4.7 níže), které pravděpodobně použije, a důvody, proč preferuje některé oblasti;*
- *Jak se bude případně provádět koordinovaný a/nebo společný dohled s jinými orgány NSA (viz oddíl o koordinovaném dohledu a spolupráci uvedený níže);*
- *Rizika na vyšší úrovni. U tohoto bodu se od orgánu NSA očekává, že uvede, jaká podle něj v systému existují nejvyšší bezpečnostní rizika a jak k tomuto závěru dospěl;*
- *U rizik na nižší úrovni se provádí všeobecný dohled. U tohoto bodu se od orgánu NSA očekává, že uvede, co považuje za rizika na sekundární úrovni, a uvede, proč k tomuto závěru dospěl.*

4.7 Techniky dohledu

Článek 4 CSM pro dohled ukládá, aby orgány NSA přijaly vhodné techniky a uvedly je při plánování svých dohledových činností. Techniky dohledu mají široký význam a jedná se jak o sběr informací (související činnost) za účelem šetření bezpečnostních výsledků systému řízení, tak přímo o specifické činnosti, např. pohovory s lidmi. Protože dohled nad železničními podniky a provozovateli infrastruktury za účelem zajistit dodržování vnitrostátního práva a práva EU z jejich strany představuje pro NSA rozsáhlý úkol, existuje analogicky mnoho různých metod, které lze použít ke sběru informací o úrovni dodržování předpisů. Součástí všech těchto metod je nicméně sběr informací různými způsoby, následovaný analýzou, co informace říkají o systému řízení bezpečnosti organizace, která je předmětem dohledu, a úrovni dodržování právních předpisů z její strany.

Existují různé specifické techniky, které lze použít k provádění dohledových aktivit na pracovišti nebo mimo ně. Patří k nim:

- *kontrola fyzického majetku na místě, např. kolejových vozidel nebo prvků infrastruktury;*
- *kontrola postupů a dokumentace pro řízení bezpečnosti, aby se zajistilo, že jsou vhodné pro daný účel;*
- *pohovory se zaměstnanci železničního podniku na všech úrovních nebo s provozovateli infrastruktury, kterými se zjišťuje, jak dobře rozumí praktickému uplatňování postupů a pravidel, a kterými se posuzuje kultura bezpečnosti organizace;*
- *audity podle definované normy systému řízení, např. OHSAS 18001:2007;*
- *audity podle modelu definovaného orgánem NSA;*
- *audity/kontroly činnosti nebo procesu po mimořádné události;*
- *audity způsobilosti/vyspělosti řízení bezpečnosti;*
- *analýzy dat;*
- *namátkové kontroly výrobků nebo činností;*
- *sledování prací (např. jízdy v kabině, kdy se sleduje chování řidiče);*
- *přítomnost orgánu NSA na důležitých jednáních managementu RU nebo IM (např. o přejezdech nebo projektech nové infrastruktury);*
- *průzkumy v organizacích vyžadující vyplnění dotazníku sebehodnocení, např. k vyhodnocení kultury bezpečnosti nebo dodržování právních předpisů či kontrolních seznamů;*
- *jiné relevantní činnosti, které zvyšují informovanost orgánu NSA o konkrétním RU nebo IM, jeho řízení bezpečnosti a kultuře bezpečnosti.*

Pro účely této příručky:

- **Inspekcí** se rozumí posouzení konkrétního a omezeného aspektu činnosti ŽP nebo PI, pověřeným způsobilým zaměstnancem vnitrostátního bezpečnostního orgánu (VBO). Účelem inspekce by mělo být dosažení souladu s evropským a vnitrostátním právem nebo ověření toho, zda to co bylo řečeno nebo zaznamenáno v dokumentech, které podporují systém zajišťování bezpečnosti, se skutečně uskutečňuje v praxi. Inspekce ve smylu tohoto procesu pak ověřuje, zda je tento proces zaveden, a prověřuje, do jaké míry funguje. Neznamená odfajfkování existence specifických dokumentů, protože to může inspektora informovat pouze o tom, že něco existuje, ale ne o tom, že je to používáno v praxi.
- ***Audity** znamenají strukturované zásahy, kdy se provádí kontrola RU nebo IM podle konkrétního standardu řízení bezpečnosti nebo podle konkrétního auditního protokolu.*
- ***Audity modelu vyspělosti a způsobilosti řízení bezpečnosti** jsou strukturovanou metodou provádění auditu systému SMS prověřované organizace za použití modelu způsobilosti/vyspělosti řízení, kterým se zkoumá, jak efektivně organizace řídí bezpečnost (viz též pokyny agentury k jejímu modelu vyspělosti řízení). Používají-li příslušní dohledoví zaměstnanci tento model správně, může poskytovat obrázek o účinnosti systému SMS.* Může proto představovat užitečný nástroj, který musí vnitrostátní bezpečnostní orgány používat k poskytování informací o fungování konkrétního systému řízení bezpečnosti při posuzování žádosti o obnovení.

Používané techniky, např. pohovory, prověrky dokumentace nebo kontrolní šetření, lze provádět do větší či menší hloubky napříč menším či větším spektrem procesů a lze je kombinovat tak, aby poskytovaly obraz o bezpečnostních kvalitách organizace a odhalovaly skryté nedostatky.

Pohovory s lidmi, kontroly dokumentace a kontrolní šetření lze následně používat k vytvoření úsudku o vyspělosti řízení organizace a schopnosti systému řídit rizika, která jí hrozí. Způsobilá osoba provádějící audit následně podle vlastního úsudku za použití modelu způsobilosti nebo vyspělosti řízení vyhodnotí, jak dobře řídí systém řízení bezpečnosti dané organizace její bezpečnost.

Sledování prací a přítomnost na jednáních managementu představují aktivity, které prohlubují informovanost orgánu NSA o konkrétním železničním podniku nebo provozovateli infrastruktury a jeho bezpečnostní kultuře.

Pro orgán NSA se jako ideální situace doporučuje kombinace dohledových technik. Každý orgán NSA se musí snažit dosáhnout rovnováhy mezi aktivitou prováděnou shora dolů (audity systému SMS) a aktivitou prováděnou zdola nahoru (prohlídkami na pracovišti, které slouží k pozorování probíhající činnosti). Dohledové metody mohou spojovat stávající činnosti v rámci prohlídek a kombinovat je s audity systému SMS za účelem náhodných kontrol mechanismů řízení. Eliminují se tak některé slabiny konkrétních technik a vytváří se tak reálnější celkový obraz o tom, jakých výsledků dosahuje předmět dohledu v praxi.

Techniky popsané výše může orgán NSA použít také k provádění horizontálních kontrol vazeb mezi železničními podniky a/nebo provozovateli infrastruktury za účelem získání celkového obrazu o tom, jak jsou různé záležitosti řízeny v celé železniční soustavě na úrovni členského státu.

Tabulka v následující části ukazuje, jak spolu souvisí obecné kontroly a audity systémů řízení, zejména techniky dotazování, kontroly dokumentace a monitorování. Tyto typy technik jsou uvedeny v normách, jako např. ISO 19011 „Pokyny pro audity systémů řízení“, a orgány NSA se mohou libovolně rozhodnout, zda se budou požadavky normy řídit či nikoli. V níže uvedené tabulce jsou vyjmenovány typy technik související s různými druhy činností.

Tabulka 1: Vztah mezi činností na místě a mimo ni při auditech a inspekcích systémů řízení

	Aktivita na pracovišti	*Aktivita mimo pracoviště*
Interakce s lidmi	vedení pohovorů vyplňování kontrolních seznamů a dotazníků za účasti auditovaného subjektu provádění kontrol dokumentace za účasti auditovaného subjektu namátkové kontroly	prostřednictvím interaktivní komunikace: • vedení pohovorů; • vyplňování kontrolních seznamů a • dotazníků; • provádění kontrol dokumentace za účasti auditovaného subjektu
Omezená/žádná interakce s lidmi	provádění kontrol dokumentace (např. záznamy, analýza dat) sledování prováděné práce provádění návštěv na pracovišti vyplňování kontrolních seznamů namátkové kontroly (např. výrobků)	provádění kontrol dokumentace (např. záznamy, analýza dat) sledování prováděných prací dohledovými prostředky, zohledňující společenské a právní požadavky analýzy dat

4.8 Plány dohledu

Plány dohledu musí zajišťovat praktickou aplikaci dohledové strategie po celou dobu trvání dané strategie. Protože plán dohledu se odvíjí od dohledové strategie, musí vycházet z rizik v dohledové strategii, u nichž se má za to, že vyžadují dohled. Plán dohledu musí rovněž klást důraz na to, jak budou fungovat vazby mezi procesem hodnocení pro účely bezpečnostní certifikace a schválení a dohledovým procesem železničních podniků a provozovatelů infrastruktury po dobu platnosti osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti, v případě potřeby pak také nutnost koordinovat s agenturou, je-li bezpečnostním certifikačním subjektem, a s ostatními orgány NSA. Plán dohledu musí obsahovat informace o procesu jeho tvorby a kontroly a vazby na dohledovou strategii, např. jak výsledky plánu způsobí změny strategie. V plánu dohledu musí být uvedeny informace o tom, u kterých železničních podniků a provozovatelů infrastruktury má být prováděn dohled v roce, k němuž se plán vztahuje, a dále důvody dohledu. V plánu dohledu musí být specifikovány prostředky, které mají být vyhrazeny pro dohled. Musí být rovněž uvedeny dohledové techniky používané během dohledu. Řeší-li plán dohledu záležitosti kolem lidských faktorů, musí se orgán NSA snažit v rámci systému SMS železničních podniků a provozovatelů infrastruktury zjistit, jak jsou tyto záležitosti řízeny.

4.9 Prosazování

CSM pro dohled stanoví v čl. 7 odst. 1, že vnitrostátní bezpečnostní organ (VBO) musí mít kritéria pro řízení případů nedodržení požadavků zjištěných v SMS železničního podniku nebo provozovatele infrastruktury a příloha 1 stanoví, že vnitrostátní bezpečnostní orgán by měl v případě potřeby přijmout donucovací opatření. Tento úkon bude záviset na tom, jaké sankce vnitrostátní právní předpisy jednotlivých členských států umožňují přijmout. V souvislosti s CSM pro dohled budou případy neplnění povinností případy, kdy SMS železničního podniku nebo provozovatele infrastruktury neplní klíčový požadavek kontroly rizik. Sankce, které může vnitrostátní bezpečnostní orgán uplatňovat, by měly být založeny na klíčových zásadách dohledu (viz oddíl 4.3). VBO musí prokázat, že jakákoli opatření, která přijme, jsou přiměřená a zaměřená na vnímané riziko. CSM pro dohled (čl. 5 odst. 2 písm. a) rozděluje otázky, na které by měl vnitrostátní bezpečnostní orgán zaměřit, na závažná porušení předpisů, a na další oblasti. Úroveň sankcí, které může vnitrostátní bezpečnostní orgán uložit, by měla odrážet míru nesouladu nebo obavy. Organizace, nad níž je prosazován dohled, musí být schopna pochopit, proč je uplatňována sankce a jak se může zlepšit. Vnitrostátní bezpečnostní orgány mohou použít jakýkoli model řízení vymáhání, který se vztahuje na hlavní zásady dohledu, s cílem poskytnout strukturovaný a transparentní postup pro přijetí donucovacích opatření podle vnitrostátního práva nebo práva EU. Za účelem pomoci vnitrostátním bezpečnostním orgánům vypracovala agentura příručku o modelu řízení prosazování, která může být používána ve spojení s různými vnitrostátními právními předpisy. (viz *pokyny agentury pro model řízení prosazování*).

5. Předávání informací o dohledu a vzájemné vazby při posuzování jednotného osvědčení o bezpečnosti a schválení vozidel

Je zřejmé, že dohled je prostředkem, kterým orgán NSA zajišťuje, aby systém SMS železničního podniku nebo provozovatele infrastruktury fungoval podle ujednání uvedených v původní žádosti o jednotné osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti. Z ustanovení čl. 17 odst. 5 směrnice (EU) 2016/798 a přílohy I CSM pro dohled je zcela zřejmé, že pokud orgán NSA v průběhu dohledu zjistí, že držitel jednotného osvědčení o bezpečnosti již nesplňuje podmínky pro jeho udělení, může osvědčení omezit či odebrat nebo požádat, aby tak učinila agentura, je-li bezpečnostním certifikačním subjektem (jedna strukturovaná metoda provádění těchto prací je uvedena v příručce agentury k modelu řízení prosazování). Podle čl. 17 odst. 7 téže směrnice, vnitrostátní bezpečnostní orgán zajistí, aby strukturální subsystémy splňovaly základní požadavky a aby mohlo být schválení provozovatele infrastruktury z hlediska bezpečnosti omezeno nebo zrušeno, pokud již nejsou splněny podmínky, za nichž bylo vydáno.

V článku 5 CSM pro dohled je popsána nutnost výměny informací získaných v průběhu dohledu s částí orgánu NSA odpovědnou za posuzování pro účely osvědčení o bezpečnosti nebo s agenturou pro účely prodloužení nebo aktualizace jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti. V tomto článku se dále uvádí, že orgán NSA musí bezpečnostnímu certifikačnímu subjektu nebo orgánu NSA pro přeshraniční infrastrukturu předat relevantní informace, obsahující minimálně:

a) *Popis závažných porušení předpisů, která mohou ovlivňovat bezpečnostní parametry nebo způsobovat závažná bezpečnostní rizika, a dalších problémových oblastí zjištěných v průběhu dohledových činností. Tyto informace lze získat z auditů, audity modelu zralosti řízení bezpečnostia kontrolních zpráv a sumarizovat pro účely opětovného posuzování;*

b) *Stav jednoho (nebo více) plánů opatření vytvořených železničním podnikem nebo provozovatelem infrastruktury za účelem odstranění závažných porušení předpisů uvedených v bodě a) a relevantních kroků, které podnikl vnitrostátní bezpečnostní orgán za účelem dohledu nad vyřešením těchto záležitostí. Tyto informace lze zjistit z následných auditů a kontrol;*

c) *Přehled bezpečnostních parametrů železničního podniku nebo provozovatele infrastruktury působícího v jeho členském státě. Tyto informace lze získat z případného modelu způsobilosti / vyspělosti řízení nebo i odborným posouzením, které hodnotí účinnost a způsobilost procesů systému řízení bezpečnosti (tj. jak dobře plní své zákonné povinnosti a průběžně se zlepšují v řízení rizik);*

d) *Stav jednoho nebo více plánů opatření vytvořených železničním podnikem nebo provozovatelem infrastruktury za účelem odstranění zbytkových problémů z předchozího hodnocení.*

Orgán NSA poskytuje bezpečnostnímu certifikačnímu subjektu informace, které jsou důležité pro to, aby bylo možné pochopit, jak dobře systém SMS funguje v praxi a zda má nějaké slabiny. Bezpečnostní certifikační subjekt pak může lépe zaměřit svoji hodnoticí činnost.

Za účelem plnění těchto požadavků musí orgán NSA zvážit, jaké informace o regulované organizaci jsou důležité podle výše uvedených čtyř bodů. U bodu a) je zřejmé, že informace musí obsahovat také záležitosti označené orgánem NSA za důležité pro řízení rizika (pomocí systému řízení bezpečnosti), a u bodu b) a d) opatření a termíny, které si strany dohodly pro řešení příslušných záležitostí buď dobrovolně samotnou organizací, nebo opatřením orgánu NSA, který od organizace vyžaduje nápravu situace. Bod c) vyžaduje, aby orgán NSA předal bezpečnostnímu certifikačnímu subjektu nebo orgánu NSA pro přeshraniční infrastrukturu nástin výsledků dosahovaných organizací v oblasti bezpečnosti. Tento krok lze provést např. prostřednictvím zprávy o dohledu provedeném v příslušné organizaci nebo předložením výstupů z modelu vyspělosti řízení organizace, který nabízí přehled relativních výsledků systému SMS.

Kromě výčtu uvedeného výše mohou i níže zmíněné faktory naznačit, které informace by mohly pomoci bezpečnostnímu certifikačnímu subjektu lépe chápat, jak systém SMS funguje:

a) *Historie různých dohledových aktivit od dříve vydaného jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti a kontrola doporučení orgánu NSA zmíněných v důsledku jeho dohledových činností. Tyto informace lze získat z dohledových plánů orgánu NSA a kontrolní tabulky doporučení orgánu NSA pro příslušný železniční podnik nebo provozovatele infrastruktury;*

b) *Přehled budoucích dohledových činností orgánu NSA plánovaných pro příslušný železniční podnik nebo provozovatele infrastruktury. Tyto informace lze získat z plánů budoucího dohledu orgánu NSA;*

c) *Výsledky sběru a analýz nehod/incidentů a stížností předložených orgánu NSA, které se vztahují k efektivitě systému řízení bezpečnosti, např. stručný přehled každé události a opatření přijatého orgánem NSA za účelem dohledu nad vyřešením zmíněných problémů. Tyto informace lze za účelem vyšetřování železničních nehod a incidentů shromažďovat a analyzovat z výroční bezpečnostní zprávy železničního podniku nebo provozovatele infrastruktury, výkazů incidentů/nehod od železničního podniku nebo provozovatele infrastruktury pro orgán NSA a také z databází nebo registrů, jako např. ERAIL;*

d) *Informace o závažných bezpečnostních rizicích uvedených při interním auditu a jiných monitorovacích činnostech železničního podniku nebo provozovatele infrastruktury, stavu plánu opatření k vyřešení problémů a opatření přijatého orgánem NSA za účelem řízení jeho provádění a efektivity od dříve vydaného jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti. Tyto informace lze shromažďovat a analyzovat z výroční bezpečnostní zprávy železničního podniku nebo provozovatele infrastruktury (tj. zprávy o aplikaci CSM na monitoring);*

e) *Informace sdělené příslušným NIB k aktuálnímu vyšetřování událostí souvisejících s aktivitami železničního podniku nebo provozovatele infrastruktury a nevyřešeným doporučením z dřívějších vyšetřování, kterými se železniční podnik nebo provozovatel infrastruktury nezabývá. Tyto informace lze za účelem vyšetřování železničních nehod a incidentů shromažďovat a analyzovat z výroční bezpečnostní zprávy železničního podniku nebo provozovatele infrastruktury, ale také z databází nebo registrů, jako např. ERAIL. V souladu s čl. 8 odst. 3 CSM pro dohled musí orgán NSA rovněž koordinovat činnost s NIB. Je nutné očekávat, že orgány NSA a NIB si budou v průběhu této koordinace předávat příslušné informace;*

f) *Popis prosazovacích opatření orgánu NSA uvedených ve vnitrostátní legislativě, která se vztahují k efektivitě systému řízení bezpečnosti a která byla podniknuta vůči železničnímu podniku nebo provozovateli infrastruktury od dříve vydaného jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti. Tyto informace se vztahují ke krokům orgánu NSA podniknutým za účelem prosadit jeho rozhodnutí, např. výzvu ke zlepšení / zákaz, pokuty, dočasná bezpečnostní opatření (ve smyslu článku 17 směrnice (EU) 2016/798);*

g) *Další informace, které orgán NSA považuje za důležité pro účely hodnocení. Další informace lze shromažďovat a analyzovat z výroční bezpečnostní zprávy železničního podniku nebo provozovatele infrastruktury a z výroční zprávy orgánu NSA.*

Obecně se očekává, že orgán NSA sdělí výše uvedené informace bezpečnostnímu certifikačnímu subjektu v okamžiku podání žádosti o prodloužení jednotného osvědčení o bezpečnosti. Rozhodne-li se orgán NSA v průběhu dohledu, že přijme prosazovací opatření, např. podá na železniční podnik trestní oznámení, a domnívá-li se, že bezpečnostní certifikační subjekt má zvážit odebrání jednotného osvědčení o bezpečnosti, musí tuto záležitost předat přímo bezpečnostnímu certifikačnímu subjektu a nečekat až do podání žádosti o prodloužení jednotného osvědčení o bezpečnosti.

To tedy znamená určitou koordinační činnost osob provádějících dohled a osob provádějících certifikaci. Je nepochybně důležité dbát na to, aby si osoby provádějící dohled a osoby provádějící bezpečnostní hodnocení předávaly relevantní informace, které umožňují příslušnému subjektu řádně řešit problémy systému SMS železničního podniku nebo provozovatele infrastruktury. Orgány NSA musí ve svých dohledových strategiích a plánech používat mechanismy, kterými tuto záležitost řídí.

V čl. 11 odst. 3 prováděcího nařízení Komise (EU) 2018/763 *[praktické mechanismy vydávání jednotných osvědčení o bezpečnosti]* se jednoznačně uvádí, že po posouzení se bezpečnostní certifikační subjekt dohodne s orgánem NSA na tom, jaké reziduální problémy z posouzení plynou a které lze nechat na pozdější posouzení během dohledu.

V případě schvalování vozidel je nutné, aby existoval také mechanismus, kterým osoby potvrzující schválení vozidel předávají relevantní informace ze schvalování vozidel osobám provádějícím dohled zejména v souvislosti s omezeními podmínek používání vozidel. Orgány NSA musí mít obdobně mechanismus, kterým osoby provádějící dohled předávají informace zpět osobám, které schválily konkrétní vozidlo, existují-li obavy o to, zda toto vozidlo stále splňuje podmínky, za nichž bylo vydáno schválení typu vozidla nebo schválení vozidla pro uvedení na trh. Pokud je tomu tak, může být v závislosti na nedostatku, vznesena bezpečnostní výstraha prostřednictvím bezpečnostního informačního systému (SIS). Vnitrostátní bezpečnostní orgán by měl rovněž přijmout opatření ke kontrole toho, jak ŽP/PI ovládá riziko a informuje ECM.

6. Koordinace orgánů NSA

Článek 8 CSM pro dohled ukládá, aby orgány NSA koordinovaly své dohledové činnosti s dohledovými činnostmi jiných orgánů NSA, probíhá-li přeshraniční provoz. Tato koordinace je nutná proto, aby se zamezilo duplikaci aktivity orgánů NSA a aby organizace, kde probíhá dohled, nebyly zatěžovány mnoha kontakty bezpečnostních regulátorů z jiných zemí. Tato koordinace probíhá také z toho důvodu, aby si různé orgány NSA dohlížející na přeshraniční provoz předávaly relevantní informace, které jim umožňují provádět efektivní dohled. V případě koordinace dohledových činností je nutné, aby si orgány NSA mezi sebou rozhodly, který z nich bude „vedoucím" orgánem NSA. V tomto kontextu je „vedoucím" orgánem NSA ten orgán, který působí jako celkový koordinátor dohledových činností a jako hlavní kontaktní osoba pro zúčastněný železniční podnik nebo provozovatele infrastruktury. „Vedoucím" orgánem NSA může být orgán NSA z členského státu, kde probíhá největší objem aktivity nebo kde je registrována organizace, nad níž probíhá dohled. Orgány NSA se musí shodnout na nejdůležitějších oblastech, které budou zkoumat v průběhu dohledu za životní cyklus jednotného osvědčení o bezpečnosti nebo schválení z hlediska bezpečnosti, a vytvoří plán plnění závazků, které si společně dohodly. Orgány NSA se musí rovněž dohodnout na rozhodčím řízení v případě sporů, které řeší neshody orgánů NSA provádějících dohledovou činnost.

Příloha II CSM pro dohled dává rámec koordinovanému a společnému dohledu, který mohou orgány NSA využívat jako vzor řízení tohoto procesu. Základní aspekty spočívají v tom, že dohled musí být koordinován tak, aby železničnímu podniku nevznikaly zbytečné problémy, např. dbá se na to, aby různé orgány NSA současně nevyžadovaly důležité zaměstnance v železničním podniku nebo aby v krátké době proběhlo na tomtéž místě více návštěv zaměřených na sběr informací. Působí-li orgány NSA podle právních norem, které nepředpokládají nebo nedovolují „společný dohled", musí být tato skutečnost reflektována ve smlouvách, které spolu uzavřely. V tomto případě je nutné, aby „vedoucí" (nebo koordinující) orgán NSA vytvořil s ostatními dotčenými orgány NSA společný plán realizace nezbytných dohledových činností v jednotlivých členských státech.

Existuje-li mezi železničními společnostmi dohoda (či smlouva) o partnerství, která umožňuje vlaku z jednoho členského státu stát se vlakem z jiného státu v okamžiku, kdy překročí státní hranici (přestože vlakový personál a vlak jsou z železniční společnosti v prvním členském státě), koordinují dotčené orgány NSA vzájemně svoji činnost a dbají tak na to, aby rizika související se záležitostmi na rozhraní mezi železničními společnostmi, např. školení zaměřené na příslušné vnitrostátní nebo mezinárodní předpisy a údržba daných vlaků, byly správně řízeny. Odhalí-li za těchto okolností jeden orgán NSA problémy v ujednáních s železniční společností, musí kontaktovat příslušný sousední orgán NSA a dotázat se jej, jaká opatření plánuje podniknout k řešení záležitosti.

Další informace naleznete v *Pokynech agentury ke koordinaci mezi orgány NSA*.

7. Lidský faktor a bezpečnostní kultura

Pro účely bezpečnostního hodnocení a dohledu musí být zaměstnanci NSA schopni odhalit lidský faktor a strategii bezpečnostní kultury a způsob, jak organizace, nad níž je prováděn dohled, integruje tyto záležitosti do svého systému SMS (viz příloha I a příloha II CSM pro SMS). V návaznosti na to by měl vnitrostátní bezpečnostní orgán vytvořit soubor poznatků o tom, jak jsou zohledněny otázky lidských faktorů a kultury bezpečnosti, které mohou být využity k formování strategie dohledu a plánu (plánů) dohledu (viz rovněž *pokyny agentury pro požadavky na SMS* a *pokyny agentury pro model splatnosti řízení*).

8. Spolupráce s jinými příslušnými orgány nebo subjekty

Předpokládá se, že orgán NSA jednající jako bezpečnostní regulátor v členském státě bude případně povinen být v průběhu výkonu svých funkcí ve styku a spolupracovat s jinými příslušnými orgány nebo subjekty.

Čl. 8 odst. 3 CSM pro dohled stanoví, že vnitrostátní bezpečnostní orgán musí vytvořit ujednání o spolupráci s příslušnými dalšími orgány, jako je NIB, certifikační orgán pro ECM, nebo s jinými příslušnými orgány, aby byly náležitě sdíleny příslušné informace a náležitě řešena závažná bezpečnostní rizika. Účelem tohoto ustanovení je zajistit, aby ti, kteří mohou potřebovat přijmout konkrétní opatření v rámci svých kompetencí, byli řádně informováni a mohli patřičně reagovat.

Může například mít potřebu spolupracovat s orgány pověřenými regulací přepravy nebezpečného nákladu, inspektorátů práce, policie (vymáhání trestního práva), regulačních orgánů v oblasti ochrany životního prostředí, subjektů odpovědných za certifikaci SOÚ, regulačních subjektů v oblasti správy železnic, orgánů vydávajících povolení nebo certifikačních orgánů a orgánů vydávajících licence.

Níže uvádíme ilustrativní výčet příkladů této spolupráce. Orgány NSA musí dbát na to, aby byly v případě potřeby odpovídajícím způsobem harmonizovány jejich strategie a plány.

8.1 Autorizační nebo certifikační subjekty

Od orgánů NSA se očekává, že budou spolupracovat s dalšími autorizačními subjekty (např. subjekty odpovědnými za schvalování vozidel) nebo případně certifikačními subjekty, např. subjekty odpovědnými za certifikaci školicích středisek pro strojvedoucí. V případě dohledu musí NSA provádějící dohled akceptovat osvědčení nebo schválení předložená jako důkaz shody s předpisy EU nebo jinými předpisy, týkají-li se záležitosti, která je předmětem dohledu. Dozví-li se NSA v průběhu dohledové činnosti, že existuje závažný bezpečnostní problém, který se týká záležitosti, u níž se předkládá schválení nebo osvědčení, musí podniknout nezbytné dočasné nápravné opatření (např. pozastavit používání vozidla) a předat záležitost příslušnému subjektu, který je odpovědný za vydání osvědčení nebo schválení.

8.2 Záležitosti bezpečnosti na pracovišti

Některé orgány NSA nesou odpovědnost za záležitosti bezpečnosti na pracovišti v rámci regulačních systémů svého členského státu, jiné NSA však nikoli. V prvním případě musí problémy s bezpečností na pracovišti, které jsou případně zjištěny v průběhu dohledu, řešit osoba provádějící dohled. Dozví-li se v druhém případě zaměstnanci NSA provádějící dohled o problémech s bezpečností na pracovišti, musí informovat organizaci, která je předmětem dohledu, že zjistili problematickou skutečnost, a musí následně předat záležitost relevantnímu příslušnému orgánu, který ji bude řešit. NSA musí rovněž podle potřeby koordinovat činnost a být ve styku s regulačním orgánem odpovědným za bezpečnost zaměstnanců, který zajišťuje harmonizaci vlastních strategií a plánů.

8.3 Pravidla pro pracovní dobu, dobu řízení a dobu odpočinku strojvedoucích

Ustanovení čl. 17 odst. 4 směrnice (EU) 2016/798 ukládá, že příslušný orgán nese odpovědnost za zajišťování shody s pravidly o pracovní době, době řízení a době odpočinku strojvedoucích. Není-li příslušným orgánem NSA, musí orgán spolupracovat s NSA a umožnit tak NSA vykonávat dohledovou činnost. Z toho plyne, že není-li NSA příslušným orgánem odpovědným za shodu s těmito pravidly, ale dozví se svými dohledovými činnostmi o problémech v konkrétní organizaci, které se jej týkají, musí při nejbližší příležitosti informovat příslušný orgán o svých zjištěních.

8.4 Spolupráce orgánu NSA a jiných regulačních subjektů

V čl. 56 odst. 3 směrnice 2012/34/EU se uvádí:

Regulační subjekt rovněž úzce spolupracuje s vnitrostátním bezpečnostním orgánem ve smyslu směrnice Evropského parlamentu a Rady 2008/57/ES ze dne 17. června 2008 o interoperabilitě železničního systému ve Společenství, a s orgánem vydávajícím licence ve smyslu této směrnice.

Členské státy zajistí, aby tyto orgány společně vypracovaly rámec pro sdílení informací a spolupráci zaměřený na předcházení nepříznivým dopadům na hospodářskou soutěž nebo bezpečnost na železničním trhu. Tento rámec bude obsahovat mechanismus, jímž bude regulační subjekt vnitrostátnímu bezpečnostnímu orgánu a orgánu vydávajícímu licence poskytovat doporučení o otázkách, jež mohou mít dopad na hospodářskou soutěž na železničním trhu, a jímž bude vnitrostátní bezpečnostní orgán poskytovat regulačnímu subjektu a orgánu vydávajícímu licence doporučení o otázkách, jež mohou mít dopad na bezpečnost. Aniž je tím dotčena nezávislost daných orgánů, pokud jde o jejich pravomoci, příslušný orgán zohlední veškerá doporučení předtím, než přijme rozhodnutí. Pokud se příslušný orgán rozhodne těmito doporučeními neřídit, uvede v rozhodnutí své důvody.

To může v praxi znamenat:

a) *V situaci, kdy regulační subjekt uloží zavedenému železničnímu podniku, aby „zpřístupnil“ služby konkurenci, ale ten odmítne a jako důvod uvede „bezpečnost“, požádá regulační subjekt orgán NSA jako „bezpečnostního regulátora“ o jeho stanovisko, zda se jedná o oprávněný důvod nezpřístupnit služby. Regulační subjekt následně zohlední stanovisko NSA při rozhodování o tom, jaké kroky podnikne;*

b) *V situaci, kdy provozovatel infrastruktury zamýšlí podat orgánu NSA žádost o schválení uvedení do provozu traťového subsystému ETCS Level 1, který používá některé volitelné funkce (např. doplňkový smyčkový či radiový přenos), kvůli nimž musí být vozidla vybavena příslušným zařízením, jinak na této trati nemohou jezdit, pak musí NSA požádat regulační subjekt o potvrzení, že tato skutečnost není diskriminační vůči železničním podnikům a že byly všem zainteresovaným stranám předány relevantní informace, aby měly čas na odpovídající úpravu svých kolejových vozidel.*

8.5 Spolupráce mezi orgánem NSA a orgánem vydávajícím licenci

Ve směrnici 2012/34/EU se uvádí:

Čl. 24 odst. 3: *Bez ohledu na odstavec 1, byla-li licence pozastavena nebo odebrána z důvodu nesplnění požadavku finanční způsobilosti,* ***může orgán vydávající licence vydat dočasnou licenci*** *platnou po dobu reorganizace železničního podniku,* ***není-li ohrožena bezpečnost****. Dočasná licence nicméně neplatí déle než šest měsíců ode dne vydání.*

Čl. 24 odst. 5: *V případě změny ovlivňující právní postavení podniku, zejména v případě sloučení nebo splynutí nebo převzetí kontroly,* ***může orgán vydávající licence rozhodnout, že licence má být znovu předložena ke schválení. Daný železniční podnik může pokračovat v činnosti, pokud orgán vydávající licence nerozhodne, že je ohrožena bezpečnost.*** *Takové rozhodnutí musí být odůvodněno.*

V praxi musí orgán vydávající licenci, který rozhoduje o vydání licence, konzultovat své kroky s NSA jako bezpečnostním regulátorem. Orgán vydávající licenci musí zodpovědět otázku, zda je pravděpodobné, že bude ohrožena bezpečnost. Požádá-li železniční podnik, aby vykonával činnost na základě dočasné licence (viz čl. 24 odst. 3). Druhou otázkou, kterou je nutné zvážit, je otázka, zda musí být ke schválení znovu podána žádost o vydání licence (viz čl. 24 odst. 5). Při rozhodování vezme orgán vydávající licenci v úvahu stanovisko orgánu NSA jako bezpečnostního regulátora.

8.6 Spolupráce orgánu NSA a subjektu pro certifikaci ECM

Orgány NSA a subjekty pro certifikaci ECM spolupracují a snaží se tak zamezit duplikaci aktivit. Jestliže se tedy orgán NSA v průběhu dohledu setká s vozidlem (nákladním vagonem), které je nekvalitně udržováno, a vzniknou tak pochyby, zda příslušný ECM dodrží podmínky, za nichž mu bylo vydáno osvědčení, sdělí tuto informaci příslušnému subjektu pro certifikaci ECM uvedenému v článku 9 nařízení ECM. Stejně tak odmítne-li subjekt pro certifikaci ECM vydat osvědčení stávajícímu ECM, musí tyto informace sdělit příslušným orgánům NSA. Tyto informace umožňují orgánům NSA upravit odpovídajícím způsobem svoji dohledovou strategii a plán.

9. Rámec řízení způsobilosti

V souladu s čl. 6 CSM pro dohled zajišťují vnitrostátní bezpečnostní orgány, aby personál zapojený do dohledu měl potřebnou odbornou způsobilost. Vnitrostátní bezpečnostní orgán by měl vybírat, školit a udržovat způsobilost těchto pracovníků prostřednictvím systému řízení způsobilosti. Je na každém jednotlivém vnitrostátním bezpečnostním orgánu, aby v souladu s čl. 6 vytvořil a vytvořil svůj vlastní systém řízení způsobilosti v souladu s nařízení o CSM. S cílem pomoci vnitrostátnímu bezpečnostnímu orgánu řídit tuto otázku připravila Agentura pokyny k systému řízení způosobilosti, přičemž tato příručka poskytne poradenství o tom, co představuje vhodný systém řízení způsobilosti, a o tom, které otázky musí vnitrostátní bezpečnostní orgán zvážit při jeho vývoji (viz *pokyny agentury pro rámec řízení způsobilosti*). Příručka však nebude přesně určovat, jaký má systém řízení způsobilosti vypadat, neboť to toto bude záležitostí jednotlivých vnitrostátních bezpečnostních orgánů.

Příloha Navrhovaný vzor dohledové strategie

Obsah