Zeitschrift: Bulletin de l'Association suisse des électriciens
Herausgeber: Association suisse des électriciens
Band: 59 (1968)
Heft: 1

Artikel: Informationsübertragung über Hochspannungsleitungen
Autor: Schönsleben, M.
DOI: https://doi.org/10.5169/seals-1057375

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 23.08.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Informationsübertragung über Hochspannungsleitungen

Vortrag, gehalten an der Diskussionsversammlung des SEV vom 20. September 1967 in Zürich,

von *M. Schönsleben*, Baden

65.011.56:621.39:621.31

Der Bedarf an Informationen, die in den Kraftwerkbetrieben ausgetauscht werden müssen, ist äusserst umfangreich und vielfältig. Es gibt elektrische Grössen, wie Spannungen, Ströme, Leistungen, Frequenzen, oder mechanische Angaben, wie Druckschwankungen, Durchflussmengen, Pegelwerte und Temperaturen. Da sind Befehle und Meldungen üblicher Art, sowie Führungsgrössen und Stellgrössen in geschlossenen Regelkreisen. Der Katalog liesse sich beliebig weiterführen. Man erkennt sofort, dass überall das grundlegende Problem auftritt, Informationen von einem Ort A zu einem davon entfernten Ort B zu übertragen. Auf welche Art die Übertragung ausgeführt wird und welche Forderungen dabei an die Übertragungseinrichtungen gestellt werden müssen, ist abhängig von den in reicher Auswahl vorliegenden Informationsarten.

Für einen Teil der Informationen wird höchste Übertragungssicherheit verlangt. Die Informationen müssen auf alle Fälle und unverfälscht zum Empfänger gelangen, wobei eventuell ein grösserer Zeitverzug in Kauf genommen werden kann. In anderen Fällen steht die Übertragungsgeschwindigkeit an erster Stelle, wobei die Information selbst vielleicht äusserst einfach aufgebaut ist. Andere Informationen müssen mit höchster Präzision, d. h. hoher Auflösung übertragen werden, wobei die Geschwindigkeit eine absolut untergeordnete Rolle spielt.

Neben dieser Vielfalt der Anforderungen von der Nachrichtenseite her, spielen auch Randbedingungen aus der eigentlichen Technik der Nachrichtenübertragung eine bedeutende, ja oft entscheidende Rolle. Es sind dies z. B. die Bandbreite, die für die Nachrichtenübertragung zur Verfügung gestellt werden kann, die Leistung, mit der die Nachrichtensender ausgerüstet werden dürfen und die Störungen mit denen auf dem Übertragungsweg und bei den Empfangsanlagen gerechnet werden muss.

Wenn man versucht diese vielfältigen Einflussgrössen etwas systematisch zu gliedern, so erkennt man, dass bei der Beurteilung einer Nachrichtenverbindung drei Punkte einer eingehenden Betrachtung bedürfen:

a) Bedingungen die der Übertragungsweg an das Übertragungssystem stellt;
b) Eigenschaften der zu übertragenden Information, und daraus folgend,
c) Wahl der Übertragungsmittel und Methoden.

1. Der Übertragungsweg

Drei verschiedene Übertragungswege stehen in vielen Fällen zur Wahl:

a) Werkeigene oder von den staatlichen Telephonverwaltungen gemietete Kabel;
b) Werkeigene Hochspannungsleitungen;
c) Mikrowellen-Verbindungen.

Bei der Entscheidung, welcher Übertragungsweg gewählt werden soll sind meistens wirtschaftliche Gesichtspunkte mit massgebend. In den folgenden Überlegungen sei nur die werkeigene Hochspannungsleitung als Übertragungsweg betrachtet und deren Vor- und Nachteile erläutert.

Ist der Übertragungsweg gegeben, muss man sich mit seinen Eigenschaften abfinden. Man muss die Übertragungsmittel und -methoden so wählen, dass sie diesen Eigenschaften entsprechen.

Der grosse Vorteil der Hochspannungsleitungen als Übertragungsweg liegt, zumindest für Elektrizitätswerkbetriebe, in der Tatsache, dass sie zwischen den Stationen, die nachrichtenmässig miteinander verbunden werden müssen, bereits vorhanden sind. Damit fallen die Erstellungs- oder Mietkosten der eigentlichen Übertragungsleitung weg. Es bleiben nur die Kosten für die Ankopplungselemente und für die Geräte. Obwohl bei hohen Spannungen und grossen Kurzschlussleistungen die Ankopplungselemente preislich stark ins Gewicht fallen, ist die Nachrichtenübertragung über eine Hochspannungsleitung bei grossen zu überbrückenden Distanzen gegenüber Mikrowellen- und Kabel-Übertragung eindeutig im Preisvorteil.

Die Hochspannungsleitung stellt an sich, obwohl sie nicht nach informationstechnischen Gesichtspunkten gebaut ist, für trägerfrequente Übertragung einen überraschend stabilen und dämpfungsarmen Übertragungsweg dar. Diesen positiven Eigenschaften stehen jedoch systembedingte, unangenehme Eigenheiten gegenüber:

Hochspannungsleitungen sind mit Leistungsschaltern und Trennern ausgerüstet. Die Betätigung von Leistungsschaltern erzeugt Störspitzen von kurzer Dauer, deren Grösse mehrere Grössenordnungen über dem durch den Koronaeffekt erzeugten Störgeräusch liegen. Noch schwerwiegender sind die Störspannungen, die bei der Abschaltung leerlaufender, kapazitiv belasteter Leitungsstücke und Sammelschienen durch Trenner entstehen.

Bei Betätigen von Trennern an leerlaufenden Leitungen können Störspannungen von über 1000 V an den Geräteeingängen entstehen, die je nach Trennerfabrikat bis zu 5 s dauern.

Die Fig. 1 und 2 zeigen solche, durch Trenner verursachte Störungen. Fig. 1 wurde direkt am Empfängereingang auf der Hochfrequenzseite aufgenommen. Die Störung dauert rund 0,7 s und es treten Spannungsspitzen von 500 V peak to peak auf. Fig. 2 zeigt eine ähnliche Störung, aber am Niederfrequenzausgang des Einseitenbandempfängers. Man erkennt, dass die Störspitzen das Nutzsignal um den Faktor 15 übersteigen.

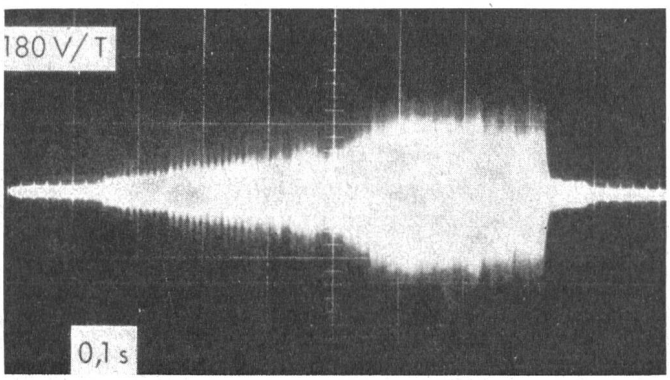

Fig. 1
Störsignal durch Trennerbetätigung
gemessen am Hochfrequenzeingang eines Einseitenband-Empfängers

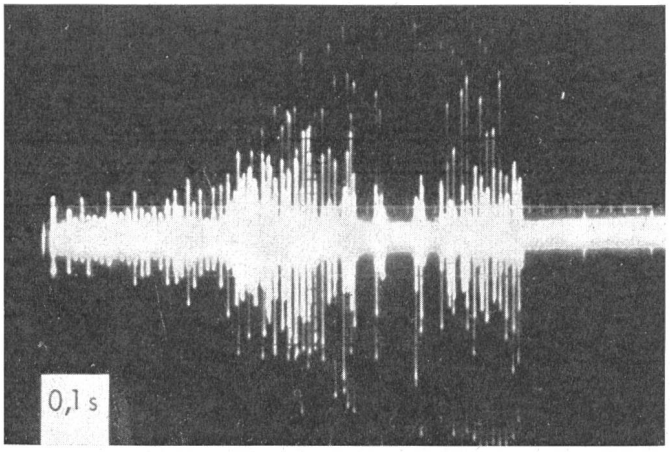

Fig. 2
Nutzsignal und Trennergeräusch
gemessen am Niederfrequenzausgang eines Einseitenband-Empfängers (vor NF-Filter)

Die Störspannungen, verursacht durch den Koronaeffekt ergeben wesentlich günstigere Signal/Rausch-Verhältnisse; die Störspitzen der Leistungsschalter sind wohl sehr intensiv, aber so kurz, dass sie sich für die Übertragung als wesentlich ungefährlicher erweisen.

Diese Bündelstörungen, von Schaltern und Trennern herrührend, wirken nicht nur über den Übertragungspfad auf den Empfängereingang. Signalleitungen, die in Kraftwerken und Unterstationen verlegt sind, können als «Antenne» wirken und induktiv oder kapazitiv angekoppelte Störspannungen von mehreren 100 V direkt auf die Mess- und Steuereingänge der Anlagen bringen. Mit diesen Tatsachen hat man sich abzufinden und auseinanderzusetzen, wenn man die Hochspannungsleitung als Übertragungsweg wählt.

2. Eigenschaften der zu übertragenden Informationen

Bei den Eigenschaften der zu übertragenden Information sind zwei Hauptkriterien zu unterscheiden:

a) Verlangte Übertragungssicherheit;
b) Maximal erlaubter Zeitverzug in der Übertragung der Information.

Die Behandlung der Information muss unter Berücksichtigung dieser Kriterien erfolgen.

2.1 Übertragungssicherheit

Ein Befehl, z. B. Steuerbefehl, darf grundsätzlich nicht falsch übertragen werden. Weil aber ein Steuerbefehl oft aufgrund ebenfalls fernübertragener Meldungen erteilt wird, gilt diese strenge Forderung auch für einen grossen Teil der Meldungen.

Ein ferngemessener und lediglich angezeigter Leistungswert, der nicht zur Leistungsregelung herbeigezogen wird, könnte unbeschadet einige Sekunden einen etwas verfälschten Wert anzeigen oder gar ausfallen. Wird derselbe Messwert aber in einem geschlossenen Regulierkreis verwendet, so kann eine solche Fehlübertragung unangenehme Folgen haben (z. B. Strahlablenkung in Hochdruckwerken).

Extrem hohe Zuverlässigkeit der Nachrichtenübertragung wird aus kommerziellen Gründen gefordert, dort wo Zählerstände von Verrechnungszählern fernangezeigt werden müssen. Es handelt sich hier um Informationen, die eventuell direkt in einen Computer eingegeben werden, der seinerseits die Rechnungstellung an die Bezüger besorgt.

Die grösste Übertragungssicherheit muss für Schutzzwecke erreicht werden. Allerdings ist hier die Nachricht äusserst einfach, besitzt sie doch nur zwei Zustände «aus» und «ein». Zudem ist der ganze Übertragungskanal nur einem bestimmten Schalter oder einer Schaltergruppe zugeordnet. Es kann daher mit einfachen Mitteln eine hohe Redundanz erreicht werden. Erschwerend wirkt aber die Tatsache, dass diese Nachrichten normalerweise bei extrem gestörten Verhältnissen übertragen werden müssen (z. B. Blitzeinschlag, Leitungskurzschluss usw.).

2.2 Zeitverzug in der Übertragung

Bei der Beurteilung des maximal erlaubten Zeitverzuges muss man sich bewusst sein, dass der totale Nachrichteninhalt und der erlaubte Zeitverzug die Telegraphiergeschwindigkeit bestimmen. Sie ist also gegeben durch die Summe der Nachrichten bei maximalem Anfall und die Zeit, die man für die Übertragung der einzelne Nachricht im Maximum zur Verfügung stellen kann. Sind alle zur Übertragung anstehenden Nachrichten gleichwertig, wie z. B. die Messwerte in einem zyklischen Fernmeßsystem, so können die Werte in einer gleichbleibenden Reihenfolge übertragen werden. Sind die Nachrichten hingegen von unterschiedlicher Wichtigkeit, so muss eine differenzierte Rangordnung dafür sorgen, dass wichtige Nachrichten, auf Kosten der untergeordneten, rascher zur Übertragung zugelassen werden. Eine Datenübertragungs- und Steueranlage muss mit einem solchen Prioritätensystem ausgerüstet sein, ansonst die Telegraphiergeschwindigkeit unnötig hoch gewählt werden müsste.

Fig. 3 fasst diese Tatsachen zusammen, wobei der Informationsgehalt einiger verschiedener Nachrichtentypen in groben Stufen angegeben ist.

3. Übertragungsmittel- und Methoden

Auf dem Gebiete der leitungsgerichteten Übertragung über Hochspannungsleitungen hat sich heute als Übertragungsmittel das Einseitenbandverfahren eindeutig durchgesetzt. Drei Gründe haben wesentlich dazu beigetragen:

a) Bandbreite ist auch auf Hochspannungsleitungen Mangelware;
b) Die Sendeleistung liegt zum grössten Teil im Nutzband (Trägerreduktion oder Trägerunterdrückung);
c) Infolge der kleineren Bandbreite werden weniger Störsignale aufgenommen.

Die Sendeleistung der Trägerfrequenzgeräte ist so gewählt, dass die am Empfänger zur Verfügung stehende Nutzspannung deutlich über dem normalen Störpegel (Koronaeffekt) der Leitung liegt, und zwar auch dann, wenn die Leitung

Art der Nachricht	Informationsgehalt			Forderung an die Uebertragung				
				Sicherheit		Geschwindigkeit		
	G	M	K	G	M	G	M	K
Fernsteuerbefehle Rückmeldungen	■			■			■	
Fernmesswerte		■			■			■
Zählerstände	■			■				■
Schutzsignale			■	■		■		

Fig. 3
Forderungen an die Übertragungseinrichtungen
G gross; *M* mittel; *K* klein

durch Schnee oder Vereisung höhere Dämpfungswerte aufweisen sollte. Gegen die hohen, bündelweise auftretenden Störungen durch Trenner und Schalterbetätigung ist auf diese Weise natürlich nicht aufzukommen. Die Sendeleistungen müssten dabei absolut unrealistische Werte annehmen. Diese Bündelstörungen müssen durch die Wahl geeigneter Übertragungsmethoden unschädlich gemacht werden. So kann man beispielsweise die im Empfänger ankommenden Signale einer Kontrolle unterziehen die anzeigt, ob eine Verstümmelung durch Störungen stattgefunden hat. Ist dies der Fall, so wird die übertragene Nachricht nicht ausgewertet. Bei Fernmessungen mit zyklischen Abtastverfahren wartet man einfach auf die nächste Übertragung, die mit grosser Wahrscheinlichkeit erst nach dem Abklingen der Störung erfolgt. Bei den Fernsteuerverfahren kann die Nachricht auf dem stets vorhandenen Rückmeldekanal nochmals angefordert werden.

Muss die Übertragungssicherheit verbessert werden, so geschieht dies daher auf Kosten der Bandbreite oder indem man einen grösseren Zeitverzug in der Übertragung in Kauf nimmt.

3.1 Codieren der Information

Es ist bekannt, dass allein schon das Codieren der Information eine Verminderung der Störanfälligkeit mit sich bringt. Voraussetzung dafür ist aber, dass die Information in digitaler Form vorliegt. So muss z. B. ein Messwert, der in Form eines Stromes am sog. Analog-Digitalwandler anliegt, in eine zu diesem Strom proportionale Zahl von Impulsen verwandelt werden. Diese Zahl von Impulsen ist nun das digitale Abbild des analogen Messwertes. Da es definitionsgemäss keine Bruchteile von Impulsen gibt, kann der Messwert nur noch in diskreten Stufen erfasst werden. Alle Zwischenwerte gehen bei dieser Digitalisierung verloren. Die Zahl der Stufen ist daher abhängig von der gewünschten Genauigkeit, mit der der Messwert am Empfangsort reproduziert werden soll. Bei einer geforderten Auflösung von 1 % benötigt man minimal 100 Stufen und bei einer Auflösung von 1 ‰ minimal deren 1000.

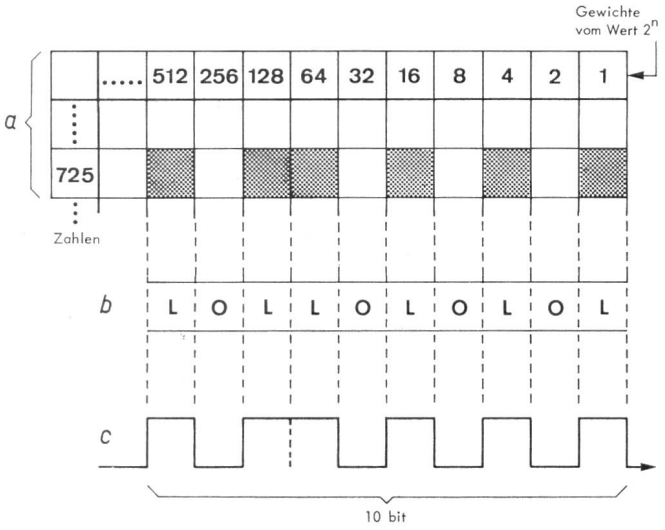

Fig. 4
Beispiel einer reinen Binärcodierung
In der Fig. ist die Zahl 725 aufgezeichnet. Diese codierte Zahl kann nun parallel (*b*) oder in Serie als Funktion der Zeit (*c*) weiterverarbeitet und übertragen werden
a Aufbau des Codes; *b* Darstellung in codierter Form; *c* Impulsdarstellung in Funktion der Zeit

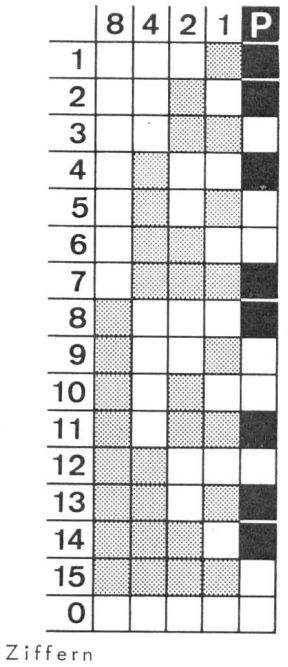

Fig. 5
Paritätskontrolle
Das P-Bit, das «gewichtslos» ist, ergänzt die Zahl der im Code vorhandenen Ja-Bit auf eine gerade Zahl

Anstelle eines analogen (ungestuften) Wertes hat man nun z. B. eine dreistellige Zahl zu übertragen. Dies kann auf zwei verschiedene Arten erfolgen, entweder dezimalziffernweise oder binär. Welche Methode die günstigere ist, hängt davon ab, was auf der Empfangsseite mit der Information gemacht werden soll. Muss ein Messwert wieder als Strom oder Spannung dargestellt werden, ist es billiger und einfacher, die Zahl rein binär zu übertragen. Soll er hingegen als Dezimalzahl angezeigt, ausgedruckt oder einem Computer übergeben werden, so ist die ziffernweise Übertragung vorteilhafter.

Fig. 4 zeigt den sparsamsten Code, den reinen Binärcode, der als bekannt voraus gesetzt werden kann. Durch Zuordnung entsprechender «Gewichte» lässt sich jede beliebige Zahl darstellen.

Die einzelnen Ja/Nein-Informationen die nach der Codierung auftreten, können alle gleichzeitig (parallel) oder zeitlich nacheinander (in Serie) übertragen werden. In beiden Fällen sind diese Ja/Nein-Informationen auf dem Übertragungsweg wesentlich weniger störbar als eine Grösse, bei der auf der Empfangsseite alle möglichen Zwischenwerte ausgewertet werden müssen.

Trotz der an sich geringen Störanfälligkeit einer Ja/Nein-Information ist es möglich, dass aus dem angegebenen Impulstelegramm auf dem Übertragungsweg ein Bit verändert wird. Damit ist die Information verfälscht, und es gibt kein Kriterium, dies festzustellen. Es ist daher unbedingt nötig, die Information gegen solche Eventualitäten zu sichern. Dabei müssen zwei Massnahmen unterschieden werden:

a) Die Fehlererkennung;
b) Die Fehlerkorrektur.

3.2 Fehlererkennung

Das einfachste Mittel zur Fehlererkennung ist die sog. Paritätskontrolle. Dabei wird die Zahl der in einem Telegrammwort empfangenen Ja-Impulse ausgezählt und festgestellt ob Geradzahligkeit vorliegt. Dies setzt voraus, dass auf der Sendeseite, unabhängig von der übermittelten Information immer eine gerade Zahl von Impulsen ausgesandt wird. Zu diesem Zweck muss eine separate, sog. Paritätskontrollstelle P im Code eingebaut werden.

Fig. 5 zeigt die Wirkungsweise dieser P-Kontrolle am Beispiel eines Binärcodes für die Zahlen 0 bis 15. Die Summe der Ja-Bit pro Wort ist immer künstlich gerade gemacht. Es ist leicht ersichtlich, dass dieses Parity-Bit nur ungradzahlige Fehler im Telegrammwort erkennen kann. Ist die Anzahl der Fehler geradzahlig spricht die Kontrolle nicht an.

Fig. 6
Aufbau des Hamming-Codes

Codestellen		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	·
Informations-Bit																							
Kontroll-Bit		P	K1	K2	J1	K3	J2	J3	J4	K4	J5	J6	J7	J8	J9	J10	J11	K5	J12	J13	J14	J15	·
Durch die Kontroll-Bit überwachte Codestellen	P	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	O	·
	K1		O		O		O		O		O		O		O		O		O		O		·
	K2			O	O			O	O			O	O			O	O			O	O		·
	K3					O	O	O	O					O	O	O	O					O	·
	K4									O	O	O	O	O	O	O	O						·
	K5																	O	O	O	O	O	·
	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·

Will man auch mehrfache Fehler in einem Telegrammwort erkennen, müssen mehrere, sich überschneidende Paritätskontrollen eingeführt werden. Dies geschieht im berühmten Hamming-Code, dessen Aufbau an Hand von Fig. 6 anschliessend erläutert sei. Es muss klar unterschieden werden zwischen den Begriffen der Codestelle, der Informations-Bit und der Kontroll-Bit. So steht das Informations-Bit J_1 an der Codestelle 4 und das Kontroll-Bit K_5 an der Codestelle 16. Das Parity-Bit P an der Codestelle 0 überwacht alle Codestellen und ergänzt falls nötig auf eine gerade Zahl. Die Kontroll-Bit K sind ebenfalls Paritätskontrollen, aber in etwas abgewandelter Art, indem sie nur für die Geradzahligkeit der L Belegungen ganz bestimmter Codestellen verantwortlich sind. So überwacht das Kontroll-Bit K_1 alle ungeraden Codestellen, das Kontroll-Bit K_2 alle «geraden Pärchen», das Kontroll-Bit K_3 alle «geraden Quadrupel» usw. Die Wirkungsweise lässt sich am einfachsten an einem praktischen Beispiel erläutern:

Codestellen		0	1	2	3	4	5	6	7
Informations-Bit					J1		J2	J3	J4
Kontroll-Bit		P	K1	K2		K3			
überwachte Codestellen	P	O	O	O	O	O	O	O	O
	K1		O		O		O		O
	K2			O	O			O	O
	K3					O	O	O	O

a

Codestellen		0	1	2	3	4	5	6	7
Informations-Bit					J1		J2	J3	J4
Kontroll-Bit		P	K1	K2		K3			
Gewicht (BCD)		0	0	0	8	0	4	2	1
Ziffern 0 bis 9	0	0	0	0	0	0	0	0	0
	1	0	L	L	0	L	0	0	L
	2	L	0	L	0	L	0	L	0
	3	L	L	0	0	0	0	L	L
	4	L	L	0	0	L	L	0	0
	5	L	0	L	0	0	L	0	L
	6	0	L	L	0	0	L	L	0
	7	0	0	0	0	L	L	L	L
	8	L	L	L	L	0	0	0	0
	9	L	0	0	L	L	0	0	L

b

Fig. 7
Hamming-Code der Ziffern 1...9
a auf 8 Codestellen (0...7) oder 4 Informations-Bit reduziertes Hamming-Schema; *b* die Ziffern 0...9 im Binärcode (4 Informations-Bit), mit 4 Kontroll-Bit nach Hamming geschützt. Hamming-Distanz $d=4$, d. h. jede Ziffer unterscheidet sich von jeder anderen durch mindestens 4 Codestellen
Weitere Erklärungen siehe im Text

Fig. 7 zeigt oben (*a*) das auf 8 Codestellen (0 bis und mit 7) reduzierte Schema der Fig. 6 und unten (*b*) die im Hamming-Code aufgezeichneten Ziffern 0 bis 9. Man sieht, dass die Gewichte der Informations-Bit rein binär abgestuft sind, (BCD-Code) und dass die Kontroll-Bit in der Reihenfolge K_3, K_2, K_1, P nach dem im Bildungschema angegebenen Verfahren gefunden werden können.

Wird nun, wie in Fig. 8 dargelegt, z. B. die Ziffer 5 codiert ausgesendet, und auf dem Übertragungsweg durch Störungen um 2 bit verfälscht, so würde die einfache Paritäts-Kontrolle versagen. Bei der Hamming-Kontrolle spricht aber das K_3 Kontroll-Bit an, weil die Summe der L-Belegungen in seinem Kontrollbereich ungerade ist.

Es lässt sich zeigen, dass alle eins, zwei- und dreifachen Fehler durch die 4 eingeführten, redundanten Kontroll-Bit eindeutig erkannt werden. Allerdings stehen in diesem Falle den 4 Informations-Bit 4 Kontroll-Bit gegenüber, und man muss sich darüber Rechenschaft geben, dass bei der Übertragung einer 3-stelligen Zahl im BCD-Code, wobei jede Ziffer für sich gegen dreifache Fehler geschützt ist, $4 \times 8 = 32$ bit benötigt werden. Legt man die drei Ziffern

Codestelle		0	1	2	3	4	5	6	7	
J- resp. K-Bit		P	K1	K2	J1	K3	J2	J3	J4	
Gewichte		0	0	0	8	0	4	2	1	
Nachricht korrekt gesendet		L	0	L	0	0	L	0	L	Ziffer 5
Störung			⬇				⬇			
Nachricht gestört empfangen		L	L	L	0	0	0	0	L	Ziffer 1
Kontrolle	P	●	●	●	O	O	O	O	●	4L, P spricht nicht an
	K1		●		O		O		●	2L, K1 spricht nicht an
	K2			●	O			O	●	2L, K2 spricht nicht an
	K3					O	O	O	●	1L, K3 spricht an

Fig. 8
Beispiel einer Übertragung der Ziffer 5, die an zwei Codestellen durch Störung verursachte Fehler aufweist
Das Kontroll-Bit K_3 spricht an. Die Störung wird einwandfrei erkannt

zu einem Wort zusammen, und schützt das ganze, zwölf Informationsbit enthaltende Wort, so benötigt man 6 Kontroll-Bit, d. h. insgesamt 18 bit. Der reine ungeschützte Binärcode kommt mit total 10 bit aus, und der ungeschützte BCD-Code braucht $3 \times 4 = 12$ bit für dieselbe dreistellige Zahl.

Eine andere, oft angewandte Methode, die ebenfalls voll gegen 1, 2 und 3-fache Fehler schützt, ist der Echovergleich. Die Nachricht, die nur ein Paritäts-Bit enthält, und somit gegen Einfachfehler geschützt wird, ist im Sender gespeichert und wird gleichzeitig zum Empfänger übertragen. Ergibt sich bei dieser Übertragung ein einfacher oder dreifacher Fehler, wird dieser von der Paritätskontrolle erkannt, und die Nachricht wird auf dem Retourkkanal neu angefordert.

Codestelle		1	2	3	4	5	6	7	
J- resp. K-Bit		K1	K2	J1	K3	J2	J3	J4	
Gewichte		0	0	8	0	4	2	1	
Nachricht korrekt gesendet		L	L	0	0	L	L	0	Ziffer 6
Störung einfach							⬇		
Nachricht gestört empfangen		L	L	0	0	L	0	0	Ziffer 4
Kontrollen	K1	●		○		●		○	Total 2L, kein Ansprechen
	K2		●	○			○	○	Total 1L, K2 spricht an
	K3				○	●	○	○	Total 1L, K3 spricht an
Korrektur einfach							⬇		
Nachricht trotz Störung richtig empfangen		L	L	0	0	L	L	0	Korrigierter Code Ziffer 6

Es haben angesprochen: die Kontroll-Bit K2 und K3, d.h. die Codestellen 2 und 4

Fehler befindet sich auf Codestelle 6 = (2 + 4)

Fig. 9
Einfach-Fehlerkorrektur mit Hamming-Code

Schleicht sich bei der Übertragung hingegen ein zweifacher Fehler ein, betrachtet die Empfangsstation die Nachricht als korrekt übertragen. Jetzt tritt der Echovergleich in Funktion, indem die empfangene Nachricht routinemässig zur Kontrolle zum Nachrichtensender zurückgesandt wird. Hier wird der Fehler erkannt, es sei denn, durch Störungen auf dem Rückweg würden beide auf dem Hinweg gestörten Bit wieder in ihre ursprüngliche Lage zurückfallen. Dies entspräche aber einem vierfachen Fehler, gegen den das Verfahren auch nicht mehr schützen kann.

3.3 Fehlerkorrektur

Ein wesentlicher Vorteil des Hamming-Codes mit Hamming-Distanzen $d \geqq 4$ liegt darin, dass er nicht nur eine Fehlererkennung, sondern auch eine nachträgliche Korrektur von Fehlern erlaubt, die sich auf dem Übertragungsweg ergeben haben. Es gilt allerdings, dass mit der Hamming Distanz $d = 4$ nur einfache Fehler innerhalb eines Codewortes korrigierbar sind. Zwei- und dreifache Fehler werden nur als solche erkannt. Die Wirkungsweise sei wieder an einem Beispiel in Fig. 9 erläutert. Für die Einfachfehlerkorrektur ist die Codestelle 0 mit dem Kontroll-Bit P nicht nötig. Sie wird daher im Schema weggelassen. Die Ziffer 6 ist in der 6ten Codestelle gestört (Einfachfehler). Dadurch wird sie in die Ziffer 4 verwandelt. Die Kontrolle K_1 die auf alle ungeraden Codestellen wirkt, spricht auf diesen Fehler nicht an. Hingegen reagieren die Kontrollen K_2 und K_3, die in deren Bereich nur ein belegtes L d. h. eine ungerade Zahl L vorfinden. Die Kontroll-Bit K_2 und K_3 liegen an den Codestellen 2 bzw. 4. Der Hamming-Code ist nun so aufgebaut, dass man die Ordnungszahlen der Codestellen ansprechender Kontroll-Bit zusammenzählen muss, um die fehlerhafte Codestelle zu finden, Beispiel: 2 + 4 = 6. Korrigiert man nun diese Code-Stelle, gewinnt man wieder Ziffer 6 zurück.

Diese Fehlerkorrektur bringt leider auch Gefahren mit sich. Bei einem Hamming-Abstand 4, d. h., wenn jede Nachricht sich von jeder anderen in mindestens 4 Codestellen unterscheidet, kann ein 3-facher Fehler durch die Korrektur in einen 4-fachen Fehler verwandelt werden, wodurch sich eine andere, zugelassene Information ergeben kann.

Ein Beispiel ist in Fig. 10 aufgezeigt, wo eine Ziffer 5 durch einen Dreifachfehler gestört, und durch eine falsche Korrektur in die Ziffer 3 übergeführt wird. Wo solche Dreifachfehler mit einer gewissen Wahrscheinlichkeit auftreten, muss man auf die Vorteile der Einfachfehlerkorrektur verzichten, oder andere Massnahmen treffen, die solche Irrtümer unschädlich machen.

Zweifachfehler können durch die Einfachfehlerkorrektur selbstverständlich nicht verbessert werden. Es sind aber auch keine Fehlinterpretationen möglich, da nach der automatisch erfolgten Korrektur eine «nicht zugelassene» Codekombination mit einer ungeraden Zahl L entsteht. Dies kann durch Auszählen der L-Bit nach erfolgter Korrektur festgestellt werden, was zur Verwerfung der Nachricht führt.

3.4 Wahl der Sicherungsmethoden

Selbstverständlich bedingt die Einführung solcher redundanter Bit eine Verlängerung der Nachricht bei gleichbleibender Information, was eine Vergrösserung des Zeitverzuges für die Nachrichtenübertragung mit sich bringt oder eine entsprechende Erhöhung der Bandbreite erfordert.

Bei der Einführung einer Redundanz zur Sicherung der Information gegen Verfälschungen auf dem Übertragungsweg muss man sich genau überlegen, auf welche Art die Redundanz eingeführt wird. Dabei ist die Kenntnis des Charakters der Störungen von grösster Bedeutung. Wenn man wieder die Hochspannungsleitung betrachtet, so wird klar, dass normalerweise, d. h. im zeitlich weitaus überragenden Teil, ein störungsarmer Betrieb vorliegt. Nur in zeitlich grossen Abständen ist mit sehr erheblichen Störungen zu rechnen. Es wäre daher wünschenswert, eine hohe Redundanz, die ja Bandbreite oder Zeit kostet, nur dann wirksam werden zu lassen, wenn Störungen vorhanden sind, und im normalen Falle mit einer bescheidenen Redundanz zu arbeiten. Da die Bandbreite, wenn sie einmal gewählt ist, nicht mehr ohne weiteres verändert werden kann, bleibt nur die Zeit oder die Sendeleistung als Variable zur Erhöhung der Übertragungssicherheit.

Bei Geräten der Schutztechnik wird oft die Leistung im Moment der Befehlsübertragung erhöht, was auch von den meisten Konzessionsbehörden erlaubt wird, da dies nur selten und sehr kurzzeitig geschieht. Bei den normalen Fernwirkgeräten aber, wo mit einer kontinuierlichen Nachrichtenübertragung gerechnet werden muss, ist diese Methode nicht gestattet. Es bleibt also dort allein die Möglichkeit, mehr Zeit für die Übertragung der Nachricht zur Verfügung zu stellen. Es ist nun ganz wesentlich, ob es gelingt, diese

Codestelle		0	1	2	3	4	5	6	7	
J- resp. K-Bit		P	K1	K2	J1	K3	J2	J3	J4	
Gewichte		0	0	0	8	0	4	2	1	
ungestörte Nachricht		L	0	L	0	0	L	0	L	Ziffer 5
Störung			⬇	⬇			⬇			
gestörte Nachricht		L	L	0	0	0	0	0	L	Ziffer 1
Kontrollen	P	●	●	○	○	○	○	○	●	P+
	K1		●		○		○		●	K1-
	K2			○	○			○	●	K2+ (Codestelle 2)
	K3					○	○	○	●	K3+ (Codestelle 4)
Korr. 2+4 = 6								⬇		
korrigierte Nachricht		L	L	0	0	0	0	L	L	Ziffer 3

Fig. 10
Gefahren der Einfachfehler-Korrektur bei Dreifachfehlern
Ziffer 5 wird durch Dreifachstörung und Einfachkorrektur in Ziffer 3 verfälscht

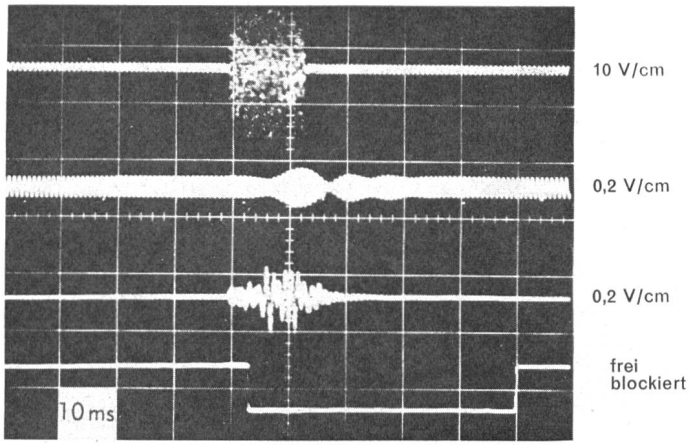

Fig. 11
Wirkungsweise des Signal-Rausch-Detektors

«Mehrzeit» nur dann einzusetzen, wenn Störungen auf dem Übertragungsweg dies erforderlich machen. Dies bedingt aber, wie später dargelegt wird, Übertragungskanäle in beiden Richtungen. Hat man nur eine Richtung für die Übertragung der Information zur Verfügung, so ist man gezwungen, sich an den schlimmsten zu erwartenden Fall anzupassen. Im Falle der Hochspannungsleitung heisst das, dass die Information auch dann übermittelt werden muss, wenn zufälligerweise gleichzeitig ein Hochspannungsschalter betätigt oder gar ein Trenner geöffnet wird. Dann ist die Störung aber derart gross und lange anhaltend, dass der Code eine äusserst hohe Redundanz besitzen müsste, sollte er die Information in diesem ungünstigen Moment unverfälscht übertragen. Nun kann aber der Nachrichtensender nicht wissen, wann Störungen solcher Art auf dem Übertragungsweg auftreten, so muss er seine Vorsichtsmassnahme zur Sicherung der Information dauernd treffen. Dies kann prinzipiell auf zwei Arten geschehen:

a) Einmaliges Übertragen der Nachricht mit einem Code, der eine Fehlererkennung *und* Fehlerkorrektur auf der Empfangsseite erlaubt, oder

b) Mehrfache Übertragung derselben Nachricht mit Identitätskontrollen oder Antivalenzkontrollen auf der Empfangsseite.

Mit beiden Verfahren wird im ungestörten Normalfall sehr viel Zeit unnötigerweise verschwendet, weil die Sicherungsverfahren stark überdimensioniert, d. h. dem schlechtesten Fall angepasst sind. Die Anwendung solcher Sicherungsverfahren ist daher nur dann sinnvoll und technisch vertretbar, wenn man nur über eine Übertragungsrichtung verfügt und somit keine Möglichkeit besteht, sich über die momentanen Verhältnisse auf dem Übertragungsweg zu informieren.

Wie bereits erwähnt, ist es weit besser, wenn es gelingt, das Sicherungsverfahren an die momentanen Störverhältnisse auf dem Übertragungsweg anzupassen. Diese Verfahren setzen aber eine zweiseitig gerichtete Verbindung voraus.

Bei gleichwertigen Verbindungen in beiden Richtungen, was bei einer Fernsteuerung normalerweise der Fall ist, kann man sich z. B. des Echovergleiches bedienen. Dabei wird die leicht redundante Nachricht ausgegeben und vom Nachrichtenempfänger zurückgeschickt. Ist das Echo, das der Nachrichtensender empfängt, in Ordnung, so wird der Ausführungsbefehl, eine hochredundante Ja/Nein-Information, übertragen. Stimmt das Echo nicht mit dem Original überein, so wird der Löschbefehl aufgegeben und die Übertragung wird wiederholt. Dies geschieht so lange, bis die Störung abgeklungen ist und die Nachricht einwandfrei übertragen werden kann.

Bei nicht gleichwertigen Verbindungen in beiden Richtungen wird die Nachricht mit einem wesentlich leistungsfähigeren, fehlererkennenden Code ausgerüstet. In der Gegenrichtung wird lediglich ein Quittungszeichen für ordnungsgemässen Empfang übertragen oder eine Aufforderung zur Wiederholung im Fehlerfall.

In beiden Fällen ist der Zeitbedarf für die Nachrichtenübertragung im normalen, ungestörten Fall gering. Erst wenn Störungen die Übertragung in Frage stellen, tritt automatisch eine hohe Redundanz in Funktion, in Form mehrfacher Wiederholungen. Eine sehr leistungsfähige Fehlererkennung muss allerdings vorausgesetzt werden.

Äusserst gute Resultate geben Verfahren, die zur Fehlererkennung eine Kombination von digitalen und analogen Störungsdetektoren besitzen. Selbst wenn eine Nachricht gegen drei oder vier Bitfehler durch Redundanz abgesichert ist, kann eine solche Sicherung bei extremen Störungen einmal überrundet werden. Die digitale Sicherungsmethode folgt ja Gesetzen der Wahrscheinlichkeit.

Wenn es gelingt, extreme Störpegel durch analog arbeitende Stördetektoren festzustellen und beim Ansprechen dieser Dedektoren die Auswertung der Nachricht vorübergehend zu sperren, so können die für die digitale Sicherung gefährlichen Fälle von der Auswertung weitgehend ferngehalten werden.

Eine solche analoge Methode wurde im sog. Signal-Rausch-Detektor realisiert. In einem Kanal, der keine Information überträgt, wird das Störsignal allein gemessen und mit dem Gemisch Nutzsignal + Störsignal im Informationskanal verglichen. Fällt das Verhältnis unter einen bestimmten Wert, wird die Auswertung der Nachricht vorübergehend gesperrt. Sobald das Verhältnis wieder eine Grösse erreicht, dass die digitale Fehlererkennung erfahrungsgemäss ausreicht, wird die Auswertung des Nutzsignales

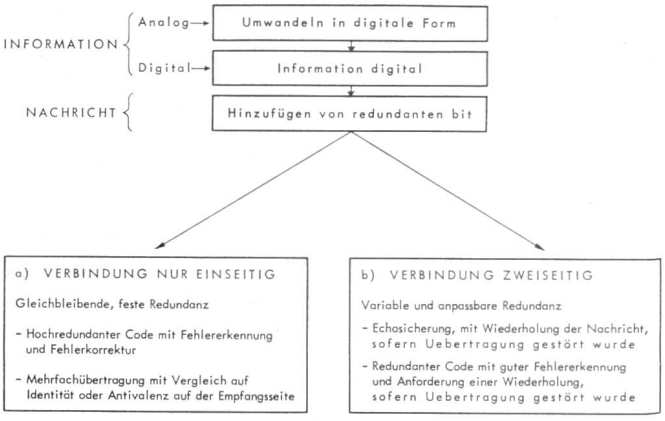

Fig. 12
Sicherung der Informationsübertragung

wieder freigegeben. Dieses Verfahren ist relativ aufwendig und wird vor allem bei Schutzaufgaben angewandt, sofern dort verlangt wird, dass eine unbeabsichtigte Schalterauslösung auch bei extremen Störungen vermieden werden muss.

Fig. 11 zeigt die Reaktion des Blockiersignales auf ein Bündelrauschen am Empfängereingang. Das Blockiersignal ist künstlich verlängert.

Bei gewöhnlichen Fernmess- und Fernsteueraufgaben wird der Signalpegel an einer geeigneten Stelle gemessen, und die Auswertung wird gesperrt, wenn das Signal ausserhalb eines festgesetzten Toleranzbandes liegt.

In Fig. 12 sind die Sicherungsmethoden als Zusammenfassung einander nochmals grundsätzlich gegenübergestellt. Nachdem die als analog vorausgesetzte Information in digitale Form verwandelt wurde, werden ihr redundante Sicherungsbit beigefügt.

Bei nur einseitiger Verbindung muss die Redundanz hoch und konstant sein. Sie ist den schlechtesten Bedingungen, unter denen die Übertragung der Information noch fehlerfrei verlangt wird, angepasst. Dabei sind zwei Möglichkeiten und deren beliebige Kombination üblich:

a) Einmalige Übertragung mit einem hochreduntanten Code, der auf der Empfangsseite eine Fehlererkennung *und* Korrektur erlaubt;
b) Mehrfachübertragung mit Vergleich auf Identität oder Antivalenz auf der Empfangsseite.

Bei zweiseitiger Verbindung kann *und soll* die Redundanz variabel gestaltet, d. h. den Verhältnissen auf dem Übertragungsweg und in der Empfangsanlage angepasst werden. Je nachdem, ob die Kapazität der Übertragungseinrichtung vom Nachrichtenempfänger zum Sender gleichwertig oder kleiner ist als diejenige in Richtung der Nachrichtenübertragung, sind zwei unterschiedliche Verfahren angebracht:

a) Bei gleichwertiger Verbindung z. B. die sog. Echosicherung mit Wiederholung der Nachricht, *sofern die Übertragung fehlerhaft war;*
b) Bei ungleichwertiger Verbindung Aussenden einer redundanten Nachricht die eine sichere Fehlererkennung auf der Empfangsseite erlaubt, mit der Möglichkeit die Nachricht neu anzufordern, *sofern die Übertragung gestört wurde.*

Man kann sagen, dass in den weitaus meisten Fällen ein Informationsfluss sowieso in beiden Richtungen erforderlich ist, so dass die Möglichkeit durchaus besteht, die momentane Qualität der Verbindung zu prüfen und sich den Gegebenheiten anzupassen. Diese Massnahme führt im Endeffekt auf eine sparsamere Ausnützung der Bandbreite, ein Ziel das immer wieder bewusst angestrebt werden muss.

Die Frage, welche von den vielen zur Verfügung stehenden Sicherungsmethoden in einem gegebenen Fall angewendet, und wie hoch die Redundanz gewählt werden soll, kann nur dann eine vernünftige Antwort finden, wenn die Besonderheiten der auftretenden Störungen durch eine sorgfältige Analyse wenigstens statistisch bekannt sind. Der Entscheid, ob z. B. ein fehlerkorrigierender Hamming-Code eingesetzt werden soll, oder ob man lediglich seine hervorragenden fehlererkennenden Eigenschaften ausnützen darf, kann nur gefällt werden, wenn bekannt ist, mit welcher Wahrscheinlichkeit auf einem Übertragungsweg Ein-, Zwei- und Dreifachfehler vorkommen. Dieser Störungsanalyse ist besondere Aufmerksamkeit zu schenken, denn ungenügende Sicherungsverfahren sind technisch unverantwortlich, und überdimensionierte Verfahren sind finanziell und bandbreitemässig unwirtschaftlich.

Adresse des Autors:
M. Schönsleben, Vorstand der Abteilung Fernwerkanlagen, AG Brown, Boveri & Cie., 5401 Baden.

Commission Electrotechnique Internationale (CEI)

32. Haupttagung in Prag vom 11. bis 25. Juli 1967 [1])

CE 12, Radiocommunications

Das CE 12 trat unter dem Vorsitz von P. Besson, Frankreich, am 11. und am 25. Juli je einen halben Tag zusammen. Es waren 13 Länder mit total etwa 25 Delegierten vertreten. Ferner waren Mitarbeiter des CCIR und der OIRT [2]) anwesend.

An der ersten Sitzung wurde das Protokoll der Tagung vom 22. Oktober 1965 in Tokio kommentarlos genehmigt. Zum Dokument *12(Secrétariat)224,* Symboles d'information pour les dispositifs de connexions et les organes de commande des appareils de radiocommunications et des équipements électroniques utilisant des techniques analogues, war eine grosse Zahl von Länderstellungnahmen eingegangen, unter anderem auch eine schweizerische Rückäusserung. Es wurde vielfach, wie von der Schweiz, die Meinung vertreten, es sollten nach Möglichkeit die vom CE 3, Symboles graphiques, genormten Symbole verwendet werden. Dem wurde allerdings entgegengehalten, der Zweck der Symbole sei hier ein anderer, nämlich dem Laien die Bedienungsorgane und Anschlußstellen kenntlich zu machen, während die Symbole des CE 3 für Verwendung in Schaltbildern durch den Fachmann bestimmt seien. Eine Detaildiskussion an der Sitzung des CE 12 war des Umfanges wegen ausgeschlossen, und die Arbeit wurde wiederum der GT 1 zur Weiterverfolgung überwiesen.

Die zweite Sitzung war der Entgegennahme der Berichte der Sous-Comités 12A, 12B und 12C gewidmet. Alle Berichte wurden genehmigt, insbesondere wurden alle Anträge zur Zirkulation von Dokumenten unter der 6-Monate-Regel für die Weiterleitung an das Comité d'Action gutgeheissen. Im einzelnen ist folgendes zu berichten:

S. A. C. Pedersen, Präsident des SC 12A, Matériel de réception radioélectrique, machte bei der Vorlage seines Rapportes speziell darauf aufmerksam, dass im Sous-Comité zum ersten Mal die Idee und der Ausdruck «Immunity» eines Fernsehempfängers gegen das Eindringen von Signalen geschaffen worden sei. Die dafür zustehende Groupe de Travail werde sich damit noch eingehender zu befassen haben. Im übrigen kündigte er an, dass er auf den 1. Juli 1968 von seinem Präsidialamt zurücktreten möchte. Die Arbeit von S. A. C. Pedersen und seine grossen persönlichen Verdienste wurden vom Vorsitzenden gebührend gewürdigt und verdankt.

Das SC 12B, Sécurité, ist in seinen Arbeiten behindert wegen fehlender Unterlagen für zulässige Betriebstemperaturen von Isoliermaterialien durch das CE 15, Matériaux isolants. Es wurde beschlossen, erneut an das Comité d'Action zu gelangen, um die gewünschten Angaben vom CE 15 zu erlangen. Das SC 12B hatte ferner mit einer schwachen Mehrheit beschlossen, elektrische Photoblitz-Ausrüstungen nicht zu behandeln. Das CE 12 einigte sich darauf, die Nationalkomitees in einer Umfrage um ihre Meinung zu bitten.

Im Zusammenhang mit dem Bericht des SC 12C, Matériel d'émission radioélectrique, wünschte ein amerikanischer Delegierter eine Abkürzung des Verfahrens bei der Bearbeitung der Dokumente, indem die Dokumente herausgegeben werden sollten, bevor alle

[1]) Eine erste Reihe der Berichte erschien im Bulletin des SEV Nr. 22 vom 28. Oktober 1967 auf den Seiten 1013...1024.
[2]) Organisation Internationale de Radiodiffusion et de Télévision.