Zeitschrift: Vermessung, Photogrammetrie, Kulturtechnik : VPK = Mensuration, photogrammétrie, génie rural

Herausgeber: Schweizerischer Verein für Vermessung und Kulturtechnik (SVVK) = Société suisse des mensurations et améliorations foncières (SSMAF)

Band: 79 (1981)

Heft: 9

Artikel: Projet pour une future norme sécurité des données dans la mensuration officielle [traduction]

Autor: Chevallier, J.J. / Durussel, R.

DOI: https://doi.org/10.5169/seals-230681

Projet pour une future norme Sécurité des données dans la mensuration officielle

Commission d'automation SSMAF: A. Frank, U. Höhn
(Traduction française: J. J. Chevallier, R. Durussel

Remarque préliminaire:
La SSMAF envisage la publication de normes. Le présent texte sur la sécurité des données correspond à l'image que se fait la Commission d'une future norme sur ce thème. De cette manière, le besoin en information est satisfait, en même temps que restent réservées les questions de compétence pour l'approbation et l'édition de telles normes.
Il convient de distinguer dans ce texte
- les parties normatives
- les commentaires y relatifs.

Les commentaires sont écrits en petites lettres.

Table des matières:

1. Notions[1]

Sécurité des données

[1] La sécurité des données comprend toutes les mesures destinées à prévenir la perte ou l'altération des données stockées, et garantissant leur accès dans un délai normal.

[3] Il convient de distinguer les notions de sécurité et de protection ou de validité.

La protection a pour but d'empêcher l'accès ou la modification des données aux tiers non autorisés. La validité des données garantit que celles-ci décrivent effectivement la réalité.

2. But de la sécurité des données

[1] Il s'agit de maintenir les données stockées par des moyens informatiques dans un état rendant possible en tout temps leur utilisation.

Les données et les moyens d'accès sont à conserver de telle manière qu'ils ne puissent être détruits ou altérés. Les données doivent de plus être en tout temps accessibles dans un délai convenable.

Il convient pour cela de s'assurer qu'en aucun cas toutes les copies de sécurité puissent être détruites ou altérées simultanément. Lors de pannes inévitables, les données originales doivent pouvoir être reconstituées.

Il faut être particulièrement attentif aux dangers suivants:

a) Des données peuvent être détruites du fait de la destruction de leur support.

b) Des données isolées ou l'ensemble d'un fichier peuvent être détruits par un traitement, quand bien même le support semble intact.

c) Des données stockées par des moyens informatiques peuvent ne plus être accessibles si les moyens d'accès (programmes et installations) sont défaillants.

Des données peuvent être altérées lors d'une transmission, ou des programmes élaborant des représentations alphanumériques ou graphiques peuvent restituer des données correctes de façon incorrecte; ces problèmes sont abordés dans la norme ...[2]

Le stockage des données de la mensuration officielle se fait de plus en plus sur des supports informatiques. Les éléments ainsi stockés ne sont plus directement accessibles à l'homme; nos sens ne nous permettent pas de déceler s'il y a des données stockées, si des données correctes sont sous une forme correcte, et si elles sont correctement mises à jour. Il s'en suit des problèmes tout particuliers pour la sécurité des données sur de tels supports. Cette norme doit présenter des règles y relatives.

Les données de la mensuration officielle représentent un capital considérable. Il faut s'imaginer à quel point il est difficile et onéreux de les saisir à nouveau si on les perd. La seule réintroduction à partir des formules de levé peut être déjà très coûteuse. S'il faut bien avouer qu'une sécurité absolue est inaccessible, il convient de trouver une solution optimale économiquement supportable.

Un optimum est atteint par des solutions combinées. A côté des solutions programmées, auxquelles on donnera en général la préférence, on peut aussi trouver des moyens conventionnels, comme:

- listes de sécurité
- instructions écrites sur le déroulement des opérations
- directives de travail impératives
- ...

3. But de la norme

[1] La norme ‹sécurité› doit préciser jusqu'à quel point des données doivent être garanties contre la perte. Cela n'est cependant pas réalisé par des prescriptions formelles de sécurité, mais bien par la présentation de mesures propres à assurer une sécurité suffisante.

Dans ce but, les principes et méthodes classiques en informatique seront adaptés aux problèmes de la mensuration officielle.

[2] Les exigences en matières de sécurité seront satisfaites, si les mesures prises garantissent une sécurité au moins équivalente à celle préconisée dans la norme.

[3] La norme doit être prise en considération, tant lors de l'étude de nouvelles applications de l'informatique en mensuration officielle, que pour l'examen d'applications existantes.

4. Domaine de validité

[1] La norme ‹sécurité› ne concerne que les données stockées sur supports informatiques, et donc dans la règle, non lisibles directement par l'homme.

[2] Elle peut cependant servir par analogie à l'appréciation de la sécurité des documents traditionnels de la mensuration. La norme vise tout spécialement l'informatique distribuée dans les bureaux de géomètre; elle peut s'appliquer par analogie aux centres de calculs.

[3] La norme se préoccupe des données qui sont nécessaires à l'accomplissement des tâches de la mensuration officielle: données ‹valides›, mais aussi ‹non encore valides› ou ‹plus valides›. Dans le cas de résultats intermédiaires, sera déterminant l'ampleur du handicap provoqué par la reconstitution après une perte éventuelle.

La durée de conservation de données périmées d'une mensuration officielle n'est par clairement fixée. Les autorités compétentes doivent donner à ce sujet des directives précises. Il s'agit de fixer, si des données périmées doivent pouvoir être reconstituées, et si oui dans quels délais.

[4] Les autorités compétentes fixent quelles données sont soumises à cette norme.

En annexe 2, on trouvera un exemple de données soumises à cette norme.

5. Bases

Les prescriptions légales ont le pas sur les indications techniques de cette norme.

---

[1] Les définitions sont à rassembler pour toutes les normes dans une norme spéciale.
[2] Voir norme ...

5.1 Bases légales fédérales

Code civil suisse:
En particulier art. 950 et titre final, art. 42 (RS 210)[3]
Ordonnance sur la mensuration parcellaire:
en particulier art. 4 (RS 211.432.2)
Directives pour l'emploi du traitement automatique des données en mensuration parcellaire:
en particulier art. 2 (RS 211.432.25)

5.2 Bases légales cantonales

Les prescriptions cantonales correspondantes sont à respecter.

5.3 Bases techniques

Emploi de l'informatique en mensuration parcellaire: rapport de la Commission d'automation de la SSMAF.

5.4 Bases techniques normatives

J. Schneider, Gefahren, Gefährdungsbilder und ein Sicherheitskonzept, Schweizer Ingenieur und Architekt, Nr. 7/80, p. 115.
Norme SIA 260: Sicherheit und Gebrauchsfähigkeit von Tragwerken (projet, 5e version de mai 1980)
Conceptions étrangères dans:
N. V. Jones, The Documentation and Checking of Computer Aided Engineering Computations, CAD 80 p. 273; (on y trouvera une abondante bibliographie avec des exemples des pays anglosaxons).
(Lors de la publication en tant que norme, le texte 5.4 sera supprimé)

6. Exigences en matière de sécurité

[1] Forme du texte: on décrira les diverses menaces (dangers) auxquelles sont exposées les données, ainsi que les mesures susceptibles de les en protéger. Les exigences en matières de sécurité seront ainsi indirectement définies.

[2] On prendra les mesures décrites, ou d'autres équivalentes, offrant la même sécurité contre les mêmes dangers.

[3] Il faut établir un *document de sécurité (plan de sécurité)* pour tout système d'ordinateur traitant des données de la mensuration officielle, et le réviser chaque année. Il doit préciser quels sont les moyens mis en œuvre pour assurer la sécurité des données. Il faut aussi définir les *responsabilités* pour l'exécution des mesures prévues. Mentionnons explicitement que les mesures techniques sont à compléter par des mesures d'organisation. Les documents correspondants sont à rédiger.

[4] Une sécurité absolue est illusoire; le *risque admis* sera décrit, et il sera précisé par qui il est supporté. On peut, le cas échéant, le couvrir en concluant une assurance.

Par risque admis, on entend les dangers ou combinaisons de dangers qui, bien qu'ils soient connus, ne sont pas combattus par les mesures prises, programmées ou conventionnelles. Exemple: des incendies simultanés dans plusieurs bâtiments séparés détruisent toutes les copies des fichiers; ce risque est extrêmement faible et peut être couru.
Il est actuellement possible de s'assurer contre presque tous les dangers tendant à la destruction physique des supports de données. Lorsqu'on évaluera si un risque est supportable, on considérera l'importance des données. On pourra accepter un risque plus grand pour des données ne servant qu'à la reconstruction d'anciens états des fichiers (données historiques), ou pour les données à buts statistiques (statistique des superficies).

6.1 Perte des données par destruction ou vieillissement du support

1re mesure fondamentale: Les données doivent être régulièrement copiées et les doubles (copies de sécurité) entreposées séparément.
Le risque est ainsi limité aux données modifiées depuis l'établissement de la copie. On peut encore le réduire par d'autres mesures, par exemple en conservant des imprimés séparément.
L'intervalle séparant l'établissement des copies est défini par
- le risque de perte
- le travail nécessaire pour la mise à jour de la copie en cas de perte de l'original
- le travail nécessaire pour réaliser la copie.

On établira au moins une copie par année; les exigences posées au chiffre 6.1.4.1 seront également prises en considération.

2e mesure fondamentale: Il faut mettre au point des procédés de mise à jour des copies. Elles sont à contrôler régulièrement, au minimum après toute modification apportée aux programmes, au système d'exploitation ou au matériel.

6.1.1 Perte du fait de dégâts dus aux éléments

Les supports de données sont très sensibles à la chaleur, aux poussières, à l'eau, etc.

1re mesure: En dehors des périodes d'emploi proprement dit, les supports de données sont à conserver dans des armoires fermées, étanches et hautement thermofuges.
2e mesure: Une copie des données (copie de sécurité) est à conserver dans un autre bâtiment, non soumis aux mêmes dangers.

6.1.2 Perte par destruction volontaire

6.1.2.1 par des tiers
1re mesure: en dehors du temps d'emploi, les supports de données sont à conserver sous clé. Pendant leur utilisation, il faut surveiller les locaux.

6.1.2.2 par le personnel
1re mesure: le personnel est à choisir soigneusement, et le travail est à surveiller.
2e mesure: Des mesures d'organisation doivent être prises pour éviter qu'une même personne puisse détruire toutes les données, copies de sécurité comprises.

6.1.3 Perte par destruction involontaire ou par désordre

1re mesure: Les supports de données doivent être entreposés avec ordre.
2e mesure: Ils doivent porter des indications sur
- leur contenu
- la date de leur création
- les bases utilisées pour cette création
- leur état de mise à jour
- le délai le plus court prévu pour son effacement
- la compétence pour l'effacement

3e mesure: Les anomalies apparaissant lors de l'emploi des supports de données doivent être notées. Le personnel doit être instruit en conséquence.

6.1.4 Perte par modification interne du support

Ce danger est variable selon le support et le mode d'écriture.
1re mesure fondamentale: Il ne faut utiliser que des supports de données répondant aux normes internationales de qualité (cf. ‹exigeances de qualité pour les supports de données› à l'annexe 3).
2e mesure fondamentale: les limites d'humidité, de température et d'empoussièrement doivent être respectées (cf. normes internationales ‹Conditions posées à l'environnement des supports de données› à l'annexe 4).

6.1.4.1 Supports magnétiques
1re mesure: Avant tout (ré-)emploi, l'état de vieillissement du support doit être contrôlé.
2e mesure: Le contenu doit être copié régulièrement – au moins une fois par année. Ceci est valable par analogie pour les copies de sécurité.
3e mesure: Il faut protéger les supports contre les champs magnétiques parasites et les charges statiques.

6.1.4.2 Cartes et bandes perforées
1re mesure: Les conditions de stockage sont à contrôler, en particulier l'humidité de l'air.
2e mesure: les cartes et bandes perforées sont à copier régulièrement.
3e mesure: Il est recommandé de conserver une copie sur un support plus sûr.

6.2 Destruction ou falsification des données dues à un traitement erroné

1re mesure fondamentale: Des copies régulières des bases de données et l'inscription immédiate des modifications survenues – tenue d'un journal ou d'un *log* – permettent de rétablir les bases de données actuelles.

[3] RS ≙ recueil systématique des textes légaux fédéraux

Il faut tendre vers des méthodes qui fixent automatiquement chaque modification sur un support de données indépendant de la base de données. De tels fichiers ‹log› peuvent être utilisés pour mettre à jour les copies conservées lors de la perte des données originales.
Si les bases de données originales sont complétées ou modifiées par d'autres données traitées et contrôlées issues d'autres supports, ces dernières peuvent être intégrées dans les fichiers ‹log›.
Les processus programmés peuvent également être remplacés par des indications inscrites sur du papier. Celles-ci doivent donner les renseignements concernant toutes les modifications effectuées. Des directives de travail obligatoires doivent assurer que ces renseignements sont sans lacunes.

2e mesure fondamentale: la plausibilité et la validité de toute la base de données sont à contrôler régulièrement. C'est par ce moyen que l'on détectera les erreurs qui se sont glissées malgré les autres mesures de sécurité. Les erreurs ainsi mises en évidence doivent faire l'objet de procès-verbaux donnant les informations sur les sources de l'erreur et sur sa correction, ainsi que sur les mesures qui sont touchées, pour éviter, dans l'avenir, ce type de faute.
Il faut ménager des redondances dans les données mémorisées afin de pouvoir dépister des modifications. Par exemple: somme de contrôle des fichiers, ‹bits› de parité.

6.2.1 Destruction involontaire par l'utilisateur

1re mesure: le personnel doit être formé avec soin et utiliser des indications d'utilisation claires et complètes.
2e mesure: les programmes doivent être conçus de telle manière qu'il est exclu que les données soient détruites par une faute de l'utilisateur.
3e mesure: l'accès aux bases de données et à leur modification sont à séparer des autres parties des programmes.
4e mesure: les opérations qui mettent les bases de données en danger, comme par exemple l'effaçage volontaire de données, ne doivent être effectuées que par des utilisateurs particulièrement qualifiés.
Les mesures, décrites en 6.1, pour lutter contre la perte de données en cas de destruction du support informatique, peuvent également aider, dans les cas extrêmes, à lutter contre ces dangers.

6.2.2 Falsification volontaire par l'utilisateur

1re mesure: des contrôles généraux, aussi appelés tests de plausibilité, doivent être intégrés dans les programmes et permettre d'empêcher l'utilisateur de travailler avec des données erronées.
2e mesure: les utilisateurs n'ont pas accès aux programmes en langage original.
Les programmes en langage original (programmes source) donnent la clef des tests de plausibilité prévus. Avec leur connaissance, il serait possible de trouver des lacunes dans les contrôles et de les utiliser de manière préméditée.
3e mesure: la documentation concernant un programme doit être divisée en une documentation spécifique à la maintenance du programme et une documentation destinée à l'utilisateur.
4e mesure: le développement et l'application des programmes doivent être séparés de manière stricte.
5e mesure: il doit être possible de retrouver en tout temps sur le fichier ‹log›, sur la base des mots de passe personnels, quel utilisateur a effectué telle modification et avec quelle version de quel programme.
Il faut promouvoir l'inscription d'annotations programmées *et* rédigées sur papier, archivées sans lacunes et de manière ordrée et permettant ce type de recherche.

6.2.3 Destruction ou falsification provenant de l'extérieur

1re mesure: l'accès à l'installation doit être contrôlé.
Les places de travail liées à l'installation et à l'accès à celle-ci doivent être surveillées depuis des places de travail occupées en permanence.
2e mesure: l'accès à distance aux installations, doit être régi par des mots de passe et des procédures d'identification, afin d'écarter les personnes non autorisées.

6.2.4 Destruction due à une force externe agissant sur l'installation

1re mesure: les installations doivent être conçues de telle manière qu'elles soient protégées au maximum contre les effets extérieurs. Les locaux concernés doivent pouvoir être fermés.
2e mesure: l'alimentation électrique doit être assurée, pour la climatisation également, si elle existe. Si nécessaire, il faut empêcher que des interruptions de courant électrique entraînent des dégâts.

6.2.5 Falsification par traitement correct de données initiales fausses

1re mesure: il faut contrôler, lors du traitement, que les données sont saisies sur les bons supports, c'est à dire sur les supports qui contiennent les données à jour.
Il faut, avant tout, promouvoir des contrôles qui peuvent être intégrés aux programmes. D'autre part, il faut mettre en place des mesures d'organisation qui empêchent que des données dépassées soient traitées à la place des données actuelles.

6.2.6 Destruction ou falsification dues à un disfonctionnement de l'installation

1re mesure: un disfonctionnement dans l'installation doit être dépisté par le système de gestion et ne doit pas conduire à la perte ou à la falsification des données.
Comme exemple: ‹read after write›, test de parité et autres.

6.2.7 Destruction ou falsification dues à des erreurs dans les programmes

1re mesure: les programmes de traitement des données et les programmes de gestion de la banque de données sont à séparer. Dans les derniers, il faut envisager des tests de plausibilité complets.
On ne peut pas encore assurer aujourd'hui que les gros programmes sont exempts de fautes. Pour augmenter la sécurité des données, les programmes doivent être conçus par blocs, d'une part ceux qui accèdent et modifient les données enregistrées et d'autre part ceux qui traitent ces données. Les derniers ne sont pas problématiques du point de vue de la sécurité des données. Les programmes qui accèdent aux données enregistrées doivent être encore divisés en parties, qui ne font que lire – ils ne mettent pas les données en danger – et celles qui modifient ou qui effacent. Des programmes uniquement lecteurs ne sont critiques que dans les systèmes à utilisateurs multiples où les données lues doivent être protégées contre des altérations pendant la transaction.
La validité des banques de données doit être maintenue, même lors d'événements inhabituels comme, par exemple, une coupure de courant électrique.
2e mesure: les modifications de la base de données doivent être structurées en transactions qui amènent la base de données d'un état de validité à un nouvel état de validité.
3e mesure: les transactions doivent être menées de telle manière que les phases intermédiaires non valides ne soient que passagères et qu'elles ne soient absolument pas accessibles aux autres utilisateurs.
4e mesure: si une procédure entraîne une modification (transaction) dans la base de données, il doit être assuré, qu'en cas d'interruption de la procédure, soit la modification a été menée à bien, soit pas du tout, c'est-à-dire que toute modification commencée est annulée avec retour à l'état antérieur.
5e mesure: les programmes doivent être entièrement examinés par l'autorité de surveillance avant leur acceptation dans la mensuration officielle.
L'autorité de surveillance peut déléguer cet examen à d'autres instances. Dans l'optique de la sécurité des données, l'examen des parties de programmes qui modifient les données est particulièrement important.
6e mesure: Il faut édicter des directives pour l'élaboration des programmes.
Des directives de programmation facilitent l'examen et la maintenance des programmes. Les autorités de surveillance doivent veiller à ce que les directives sont bien en possession des adjudicataires de tâches de programmation.

6.3 Accès impossible aux données par panne des mécanismes d'accès

Ce n'est pas seulement lorsque les données ont disparu d'un support de données qu'elles sont perdues, mais c'est aussi lorsque les installations, qui étaient capables de lire ces supports, ne fonctionnent ou n'existent plus.

1re mesure fondamentale: les données doivent, au moins pour les copies de sécurité, être sur des supports standards dans des formats standards. A ce propos, des normes pour l'organisation des interfaces doivent être suivies.

Les installations et les supports de données qui ne permettent pas un transfert de données sur des supports standardisés, n'offrent pas une sécurité suffisante.

6.3.1 Accès impossible par perte du logiciel d'accès

1re mesure: des copies de sécurité concernant le logiciel doivent aussi être faites et stockées de manière séparée

2e mesure: la documentation des programmes doit contenir toutes les indications qui permettent, le cas échéant, de rétablir les programmes permettant la lecture des données.

6.3.2 Accès impossible dû à la panne des installations d'accès

1re mesure: la maintenance des installations doit être assurée par contrat.

2e mesure: il faut rechercher à ce que les données puissent également être lues sur une autre installation voisine. L'utilisation de cette installation ‹étrangère› doit être convenue à l'avance avec son propriétaire. Le logiciel nécessaire à cette opération doit être élaboré et testé régulièrement.

6.3.3 Accès impossible à cause du personnel

1re mesure: les programmes pour le traitement des données doivent être documentés de telle manière à ce que toute personne initiée à l'informatique puisse les mettre en marche.

2e mesure: en plus d'une organisation interne des remplaçants du personnel, il faut prévoir des mesures équivalentes à l'aide de personnel externe.

6.4 Dangers envisageables

[1] Les dommages ne se produisent pas seulement à cause d'événements isolés. Il faut également considérer des combinaisons d'événements malheureux.

[2] Les mesures prises doivent au moins contrer les combinaisons d'événements malheureux suivants:

A) Perte des données par destruction du support de données
- due à un dommage élémentaire ou
- par destruction
  - par un tiers ou
  - par le personnel propre,

combiné avec
accès impossible aux données dû à la panne des mécanismes d'accès
- à cause d'une défaillance des programmes et/ou
- à cause d'une panne de l'installation.

Pour la remise sur pied, il faut compter également avec une désaffection du personnel.

B) Destruction accidentelle des données
simultanée avec
non-fonctionnement des programmes

C) Destruction des données par manipulation erronée simultanée avec
accès impossible aux données par panne des mécanismes d'accès. Les deux étant provoqués soit par la destruction de l'installation ou le non-fonctionnement des programmes.

7. Description des domaines de responsabilité

[1] Pour se protéger contre des dommages, il est important de définir clairement l'étendue des diverses responsabilités. Dans ce qui suit, les domaines de responsabilité et les fonctions y relatives sont décrites.

[2] Le document de sécurité des données de chaque installation (voir chiffre 6.) pose par écrit et de manière fixe les domaines de responsabilité. En plus, chaque fonction est attribuée à une personne responsable. Il faut décrire en détail tout domaine de responsabilité qui s'écarterait de la norme.

Pour les dommages, dus à la perte ou à la falsification des données, c'est, vis-à-vis de l'extérieur, le géomètre ingénieur breveté adjudicataire, éventuellement la firme de mensuration, qui est responsable. Les prétentions dues à la responsabilité légale peuvent être diminuées s'il peut être prouvé après coup que les précautions exigibles avaient été prises.

Pour la réparation des dommages, c'est au géomètre à œuvrer lui-même. A la rigueur, il peut se retourner contre un employé coupable. La fonction des autorités de surveillance du canton et de la confédération est indiquée dans les lois, en particulier dans l'IAMP 1919 SR 211.432.23. Cette fonction ne peut pas être traitée par une norme.

7.1 L'ingénieur-géomètre responsable

[1] Il est globalement responsable du respect des prescriptions légales et des mesures prévues par cette norme. En particulier, il doit:

A) établir le document de sécurité et le contrôler régulièrement,

B) délimiter les domaines de responsabilité,

C) distribuer aux collaborateurs aptes à les recevoir, les diverses fonctions définies plus loin (voir 6.1.2.2[1]),

D) instruire correctement ses collaborateurs et contrôler l'application des instructions (6.1.2.2[2], 6.2.1[1]),

E) régler la question des suppléances des postes de travail (6.3.3[2]).

Dans l'annexe 2, un exemple issu de la pratique est donné. Voir aussi l'annexe 1.

7.2 Fonction: sécurité des données à long terme

[1] Cette fonction contient les mesures 6.1, 6.1.1(1), 6.1.1(2), 6.1.2.2(2), 6.1.3(2), 6.1.4, 6.1.4.1, 6.1.4.2, 6.2(2), 6.3, 6.3.1, 6.3.2(2).

On considère ici toutes les mesures (surtout périodiques) indispensables à la sécurisation des données à long terme.

7.3 Fonction: sécurité permanente

[1] Cette fonction comprend les mesures 6.1.1(1), 6.1.2.1(1), 6.1.2.2(2), 6.1.3, 6.1.4, 6.1.4.1, 6.1.4.2, 6.2(1), 6.2.2(5), 6.2.3, 6.2.4, 6.2.5, 6.3.1(1).

On considère ici les mesures qui protègent les données contre une perte dans l'utilisation journalière. Il lui appartient en particulier de contrôler que les supports de données sont rangés avec ordre.

7.4 Fonction: entretien de l'installation

[1] Cette fonction comprend les mesures 6.1.3(3), 6.3.2(1).

La personne apte, choisie pour cette fonction, opère elle-même l'entretien ou le supervise.

Pour l'entretien des installations, il est conseillé de passer des contrats complémentaires à long terme avec le constructeur, respectivement avec le représentant.

7.5 Fonction: élaboration et maintenance des programmes

[1] Cette fonction comprend les mesures suivantes: 6.2, 6.2.1, 6.2.2, 6.2.5, 6.2.6, 6.2.7, 6.3.1(1), 6.3.3(1).

Ces mesures doivent être considérées lors de la création et de l'élaboration des programmes. Par l'examen des programmes, ceci sera contrôlé.

7.6 Fonction: utilisation de programmes ‹dangereux›

[1] La personne apte qui exerce cette fonction obtient le droit d'utiliser des programmes dangereux au sens de 6.2.1(4).

[2] Elle doit être instruite des dangers spécifiques et formée de manière particulièrement soignée (6.2.2[5]).

[3] Elle touche les mesures 6.1.3(2), 6.1.3(3).

Certains programmes, en particulier des routines du système d'exploitation, peuvent rendre inutilisables des fichiers entiers (par effacement, par exemple).

Ces programmes ne contiennent aucune sécurité contre un emploi erroné; ils ne doivent pas être disponibles sans restriction, mais être réservés aux personnes spécialement formées.

7.7 Fonction: utilisation des programmes qui modifient les données

[1] Cette fonction comprend le droit d'utiliser des programmes qui modifient la base de données.

[2] Pour cette fonction, il faut considérer des collaborateurs instruits et expérimentés, qui sont également formés pour agir dans des cas spéciaux.
[3] Elle touche les mesures 6.1.3(2), 6.1.3(3), 6.2(1), 6.2.2(5).
Les programmes de cette catégorie servent à modifier certaines données isolées; les fautes de manipulations, rendant sous contrôle du programme inutilisables une grande partie des données, sont rendues impossibles.

7.8 Fonction: utilisation de programmes qui lisent des données
[1] Les personnes aptes, qui exercent cette fonction, ont l'autorisation d'utiliser les programmes qui lisent mais ne modifient pas les données.

[2] Ces collaborateurs doivent être instruits exactement et contrôlés régulièrement. Le danger de manipulations erronées éventuelles doit être porté à leur attention.

Annexes

1. Exemple d'un document de sécurité
2. Tableau des rapports entre mesures et fonctions
3. Exigences de qualité pour les supports de données
4. Conditions environnementales pour la conservation de supports de données

Naturschutz und Landwirtschaftliche Meliorationen

W. Flury

- Meliorationen sollen der *Landwirtschaft* im Sinne ihrer Gesamtbedeutung *dienen;*
- Auf die *Belange der Orts- und Regionalplanung, des Natur- und Heimatschutzes sowie der Umwelt* ist Rücksicht zu nehmen;
- In einem *Inventar* (z. B. der zu schützenden Gebiete) können die Anliegen des Natur- und Heimatschutzes zuhanden der Vorstände der Meliorationsgenossenschaft und der betreffenden Gemeinde(n) in Bericht und Plan dargelegt werden;
- Schützenswerte Gebiete haben eine *wichtige Funktion* im Beizugsgebiet;
- *Fragen des Verfahrens* zur Erhaltung schützenswerter Gebiete im Rahmen von Meliorationen richten sich nach dem einschlägigen kantonalen Recht, die entsprechenden Grundlagen für einen sinnvollen Schutz – auch im Interesse der Landwirtschaft – sind im Bundesrecht vorhanden;
- Eine *Wegleitung* zur Beachtung des Natur- und Heimatschutzes bei Meliorationen wird zur Zeit durch eine Arbeitsgruppe vorbereitet;
- Wesentlich ist die *Zusammenarbeit* auf den Stufen Gemeinde, Kanton und Bund, wobei der Ablauf auf den Ebenen von Gemeinde und Kanton entscheidend für das Gelingen des Werkes ist.

- *Les entreprises d'améliorations foncières doivent* servir *les intérêts de* l'agriculture *dans son importance globale;*
- *Il y a lieu de respecter* les intérêts du plan d'aménagement local et régional, ainsi que de la protection de la nature, du paysage et de l'environnement;
- *Un* inventaire *(p. ex. des régions à protéger) établi sous forme d'un rapport et plan à l'attention des comités directeurs du syndicat d'amélioration foncière et de la commune ou des communes intéressées pourrait définir les intérêts spécifiques de la protection de la nature et du paysage;*
- *Les zones dignes de protection remplissent une* tâche importante *dans le périmètre;*
- *Le* procédé à suivre *pour la conservation de zones dignes de protection dans le cadre d'améliorations foncières est déterminé par le droit cantonal correspondant. Le droit fédéral contient les bases nécessaires à une protection raisonnable, compte tenu entre autre des intérêts de l'agriculture;*
- *Un groupe de travail est en train d'élaborer un* guide *pour la sauvegarde des intérêts de la protection de la nature et du paysage dans les entreprises d'améliorations foncières;*
- *Il est essentiel qu'une étroite* collaboration *existe entre commune, canton et Confédération. Pour la réussite d'une entreprise d'améliorations foncières, le déroulement des opérations au niveau communal et cantonal est décisif.*

I. Vorerst sei die *Zielsetzung* der Meliorationen und damit auch der Güterzusammenlegungen im Sinne des Landwirtschaftsgesetzes, der Bodenverbesserungsverordnung und des fünften Landwirtschaftsberichtes des Bundesrats kurz in Erinnnerung gerufen:
Neben der Verbesserung der *Produktivität* sind die *Erhaltung* des landwirtschaftlich nutzbaren Bodens, sein *Schutz* vor Verwüstungen durch Naturereignisse sowie die *Bewirtschaftung* und *Pflege* des Bodens als Teil der Landschaft anzustreben; zudem soll auch eine ausreichende Besiedlung der Berg- und Randgebiete der Schweiz gewährleistet bleiben.
In diesem Sinne erfolgen landwirtschaftliche Bewirtschaftung und Meliorationen seit Jahren in einer sich wandelnden Kulturlandschaft.
Träger der Meliorationen sind – je nach Art der vorgesehenen Massnahme (vom einfachen Wegebau bis zur umfassenden Güterzusammenlegung) – ein einzelner Landwirt, eine Genossenschaft der Beteiligten oder auch eine bzw. mehrere Gemeinden. Die Massnahmen sollen heute – gezielt und auf *Schwerpunkte* beschränkt – wie auch spartanisch und massvoll (d. h. nicht perfektionistisch) durch den Träger gemeinsam mit dem beauftragten Ingenieur und den zuständigen kantonalen Behörden disponiert und auch realisiert werden.

II. Im Rahmen der Vorbereitung und Durchführung etwa einer Güterzusammenlegung sind – im Sinne von Landwirtschaftsgesetz und Bodenverbesserungsverordnung des Bundes – neben den landwirtschaftlichen und agrarpolitischen Interessen auch die Belange der *Umwelt* zu berücksichtigen; Art. 79 des Bundesgesetzes über die Förderung der Landwirtschaft lautet:

‹Den allgemeinen Interessen der Umwelt, insbesondere der Erhaltung des Grundwassers und der damit verbundenen Trinkwasserversorgung sowie dem Schutze der Natur und der Wahrung des Landschaftsbildes ist Rechnung zu tragen.
Auf die Interessen der Fischerei, der Jagd und der Bienenzucht sowie auf den Schutz der Vögel ist Rücksicht zu nehmen.›