eurolab

Evropská federace národních sdružení měřicích, zkušebních a analytických laboratoří

Technická zpráva č. 2/2006
Říjen 2006

Technická zpráva

POKYNY PRO MANAGEMENT POČÍTAČŮ A SOFTWARU V LABORATOŘÍCH SE ZŘETELEM K NORMĚ ISO/IEC 17025:2005

Impresum

EUROLAB Technická zpráva 2/2006
„Pokyny pro management počítačů a softwaru v laboratořích se zřetelem k normě ISO/IEC 17025:2005“
(Guidance for the Management of Computers and Software in Laboratories with Reference to ISO/IEC 17025:2005)

Říjen 2006

EUROLAB Technický sekretariát
c/o Laboratoire National de Métrologie et d’Essais – LNE –
1 rue Gaston Boissier – 75015 – France
Tel.: +33 (1) 40 43 39 45
Fax.: +33 (1) 40 43 37 37
Email: mailto:eurolab@lne.fr

Pokyny pro management počítačů a softwaru v laboratořích se zřetelem k normě ISO/IEC 17025:2005

Předmluva

Tato směrnice je určena laboratořím jako pomůcka pro řízení práce se softwarem a počítači se zřetelem k požadavkům normy ISO/IEC 17025* [1]. Pracovní skupina byla složena ze zástupců akreditovaných orgánů a organizací zabývajících se posuzováním shody, profesních organizací laboratoří, ale též certifikačních orgánů, inspekčních orgánů a metrologických institucí. Členy pracovní skupiny byli: Greg Gogates (A2LA), Hugo Eberhard (CEOC), Per Lang Pedersen (EA), Steve Ellison (EURACHEM), Anita Schmidt (EUROLAB), Maria Elisa Abrantes da Costa (EUROLAB), Magnus Holmgren (EUROLAB a NORDTEST, předseda), Tanasko Tasić (EUROMET), Jan Hald (EUROMET a NORDTEST).

Rámec působnosti skupiny byl potvrzen technickou komisí EUROLAB pro zajišťování kvality. Skupina zahájila činnost během podzimu 2003.

1. Úvod a způsob použití pokynů

Úkolem skupiny bylo vytvořit stručnou a zevrubnou směrnici především zaměřenou na zvládnutí požadavků, které se specificky vztahují na počítače a software se zřetelem k normě ISO/IEC 17025. Dokument neurčuje nejlepší praxi ani komplexní řešení, nýbrž předkládá pokyny a vodítka bez závazných partií.

Je důležité si uvědomit, že zavedení informačních technologií – IT, počítačů a softwaru do procesů zkoušení a kalibrace vyžaduje určitý výklad. Autoři se shodli v názoru, že zavedení těchto technologií ve svém celkovém účinku zlepšuje kvalitu laboratorních služeb.

Pokyny předpokládají, že laboratoř pracuje v souladu s ISO/IEC 17025, tj. že má vzdělané a zkušené pracovníky, postupy pro školení a pro údržbu zařízení, koncepce a postupy pro řízení přístupu k informacím a jejich aktualizaci, postupy pro správu dokumentů apod. Mnohé otázky týkající se zabezpečení, např. elektronického přenosu, zkušebních zpráv, závisejí více na tom, co bylo ujednáno ve smlouvě mezi laboratoří a zákazníkem, než na tom, co je uvedeno v normě.

Tento dokument odráží stav, kdy počítače používané v laboratoři slouží k těmto rozmanitým účelům:

- jako prostý psací stroj, včetně tisku a uchovávání výstupů,
- vypracování a správa provozní příručky a standardních pracovních postupů, organizačního schématu, osobních dat, školení pracovníků apod.,
- předávání dokumentů prostřednictvím intranetu,
- archivace dokumentů,
- databáze zákazníků,
- řízení přístrojů,
- používání funkčně jako přístroje,
- vyhodnocování výsledků zkoušek,
- vedení grafů řízení kvality a kalibračních křivek,
- jako interní informační a řídicí systém laboratoře,
- vyhotovování zkušebních zpráv,
- internet jako externí zdroj informací,
- kontakty se zákazníky (např. prostřednictvím elektronické pošty),
- prezentace organizace na webové stránce …

Aby bylo možné vykonávat takto široký okruh činností, je třeba identifikovat opatření laboratoře potřebná k řízení kvality jejích počítačů a softwaru a vyhodnotit je z hlediska rozsahu používaných IT a rizik, která jsou s tím spojena. K tomuto účelu nabízejí tyto pokyny příklady v tabelární formě, které laboratořím umožní rozhodovat o opatřeních přijímaných případ od případu.

Činnosti a záležitosti, které vyžadují řízení pomocí IT v rámci systému řízení laboratoře se zřetelem k normě ISO/IEC 17025, lze rozdělit do dvou skupin:

* Národní poznámka: Českou verzí této normy je ČSN EN ISO/IEC 17025 (listopad 2005) „Posuzování shody – Všeobecné požadavky ne způsobilost zkušebních a kalibračních laboratoří.

a) všeobecné činnosti laboratoře, které je třeba řídit podle normy obecně, ať již jsou vykonávány s počítačovým systémem nebo bez něj; pro tyto činnosti musí laboratoř definovat politiku a postupy. V případě používání počítačového systému musí tento splňovat systémové požadavky;

b) speciální požadavky, které musí splňovat používaný software a systémy. Software a počítačový systém musí být validovány a/nebo ověřovány.

Předpokládá se, že laboratoř má opatření, která umožňují dostát obecným požadavkům ISO/IEC 17025. Proto se tyto pokyny zaměřují na speciální požadavky týkající se validace softwaru a počítačového systému a zahrnuje:

- identifikaci a interpretaci článků ISO/IEC 17025, které se týkají počítačů a softwaru (**kapitola 3**),
- zavádění počítačových systémů v laboratoři (**kapitoly 4, 5 a 6**),
- různé kategorie softwaru (**kapitola 4**),
- hodnocení rizika včetně zabezpečení (**kapitola 5**),
- ověřování a validace softwaru (**kapitola 6**),
- zpracování, přenos a archivace elektronických dokumentů (**kapitola 7**),
- odkazy (**kapitola 8**),
- osvojení IT (**příloha 1**),
- používání počítačových sítí ve spojení s procesem měření (**příloha 2**),
- zabezpečení (**příloha 3**).

Pokyny lze použit tímto způsobem:

Kapitola 3 je pomůckou, která má laboratořím pomoci identifikovat a interpretovat v normě články, jež se přímo i nepřímo vztahují k používání softwaru, počítačů, počítačových systémů a počítačem podporovaných systémů řízení kvality.

Kapitoly 4, 5 a 6 společně podávají návod k zavádění počítačových systémů v laboratořích. **Kapitola 4** je vodítkem pro kategorizaci různých typů softwaru od volně prodejného softwaru (OTS) až po programy sestavené na zakázku (CMP). Tato kapitola spolu s tabulkou 2 podává návod na způsob kategorizace softwaru. Tato kategorizace pak pomáhá laboratořím rozhodovat o způsobu správy softwaru a jeho validace.

Kapitola 5 spolu s přílohou 3 obsahuje stručný úvod ke způsobu odhadování rizik, která jsou spojena s určitým softwarem nebo počítačovým systémem, a ke způsobu, kterým může laboratoř řešit otázky zabezpečení. Navrhovaná opatření týkající se zabezpečení, obsažená v této kapitole, nejsou normou přímo požadována, jsou spíše návodem, jak řešit potenciální problémy.

Kapitola 6 podává přehled různých typů softwaru/počítačových systémů a identifikuje s nimi spojené třídy rizika. Udává rozsah, v jakém je nutná validace a/nebo testy před používáním systém IT pro akreditované činnosti. Na zvláštních tabulkách je uveden popis příslušných různých typů validace a testů.

Kapitola 7 pojednává o problematice zacházení s elektronickými dokumenty.

Příloha 1 třídí rozsah činností IT laboratoře na činnosti vyžadující vysoké, střední a nízké požadavky na řízení IT u různých článků normy ISO/IEC 17025.

Příloha 2 obsahuje pokyny pro zacházení se sítěmi ve spojení s procesem měření, založené na výsledcích projektu „software podle MID“, jehož předmětem je používání softwaru a IT u měřicích přístrojů, na které se vztahuje nová směrnice EU o měřidlech „Measuring Instruments Directive (MID)“*.

Příloha 3 (spolu s kapitolou 5) pojednává o otázkách zabezpečení a o způsobu, jakým může laboratoř tyto otázky řešit.

* Národní poznámka: Směrnice Evropského parlamentu a Rady 2004/22/ES ze dne 31. března 2004 o měřidlech, která byla převzata do nařízení vlády č. 464/2005 Sb.

2. Termíny a definice

2.1 **Počítačový systém:** Systém obsahující jeden nebo více počítačů, periferních zařízení a s nimi spojené softwarové produkty [2].

2.2 **Ověřování:** Potvrzení zkoumáním a poskytnutím objektivních důkazů, že byly splněny specifikované požadavky [3]. V těchto pokynech je ověřováním např. kontrola počítačového systému, akceptační testy uživatele a přezkoumávání kódů.

2.3 **Validace:** Potvrzení zkoumáním a poskytnutím objektivních důkazů, že jsou splněny zvláštní požadavky na specifické zamýšlené použití [1, 3]. Rozsah potřebné validace závisí na zamýšleném použití.

2.4 **Elektronický záznam:** Jakákoli kombinace testu, grafiky, dat, audia nebo jiné reprezentace informací v digitální formě, vytvořená, modifikovaná, udržovaná, archivovaná, vyhledaná nebo distribuovaná počítačovým systémem [4].

2.5 **Ochrana záznamů:** Zajištění autentičnosti, integrity a důvěrnosti po celou dobu existence záznamu. Zahrnuje prověřovací záznamy a elektronické podpisy.

2.6 **Zabezpečení záznamů:** Rozsah, v jakém je soubor dat chráněn před ohrožením náhodnou nebo svévolnou změnou nebo zničením [2].

2.7 **Migrace, přesunutí počítačového systému včetně prvotních dat z jednoho počítačového prostředí do jiného.**

2.8 **Zálohování záznamů:** Systém, součástka, soubor, postup nebo osoba, která je k dispozici, aby nahradila nebo pomohla obnovit prvotní položku v případě poruchy nebo havárie z vnější příčiny [2].

2.9 **Elektronický zdroj, záznamy o kvalitě a technické záznamy bez uchovaných originálů vytištěných na papíře.**

2.10 **Softwarový produkt:** Kompletní sada počítačových programů, postupů, popřípadě včetně doprovodné dokumentace a dat, určená k dodání uživateli. Je zaveden do hardwarového prostředí, kde se stává součástí systému v rámci managementu konfigurace [2].

2.11 **Otevřený systém:** Prostředí, ve kterém přístup do systému není pod kontrolou osob, jež jsou odpovědné za obsah elektronických záznamů, které v dotyčném systému jsou (např. internet) [5].

2.12 **Uzavřený systém:** Prostředí, ve kterém přístup do systému je pod kontrolou osob, jež jsou odpovědné za obsah elektronických záznamů přítomných v dotyčném systému [5].

2.13 **Iniciátor revalidace:** Software vyžaduje revalidaci, jestliže se změní počítačový systém (např. software) nebo požadavky. Stačí, jestliže se validace zaměřuje na příslušné funkce a počítačová rozhraní.

2.14 **Elektronický prověřovací záznam:** Zabezpečený, počítačem generovaný a časovým údajem označený elektronický záznam, který umožňuje rekonstrukci sledu událostí týkajících se vytvoření, modifikace a vymazání elektronického záznamu [4].

2.15 **Relace uživatele:** Ohraničená přiměřená doba, po kterou operátor aktivně používá počítačový systém. Po jejím uplynutí relace končí a iniciují se prověřovací záznamy. Výměnou uživatele se současná relace automaticky ukončuje.

2.16 **Zkušební software:** Software v počítačovém systému používaný ke zkoušení, kalibraci nebo vzorkování.

2.17 **Software dokumentů:** Software v počítačovém systému používaný k řízení správy dokumentů, managementu smluv, nákupu, stížností, neshod, nápravných opatření, přezkoumání systému managementu, preventivních opatření, auditů, záznamů, rozvoje odborné způsobilosti, zpráv a přenosu výsledků.

2.18 **Kontrola integrity souborů:** Přezkoumání softwarového produktu nebo souborů dat zavedených do počítačového systému za účelem potvrzení, že se soubory nezměnily (souvisí s body 5.5.10 a 5.6.3.3 normy ISO/IEC 17025).

2.19 **Akceptační test:** Formální test, který se provádí ke zjištění, zda počítačový systém splňuje specifikované požadavky, a který pomáhá laboratoři určit, zda má systém převzít.

2.20 **Specifikace požadavků:** Definice toho, co se od počítačového systému požaduje v konkrétním zamýšleném použití.

2.21 **Testování metodou black box:** Způsob testování softwaru, kdy zkoušející osoba nezná interní fungování testovaného subjektu. Též se nazývá funkční testování.

2.22 **Testování metodou white box:** Způsob testování softwaru při znalosti interního fungování testovaného subjektu. Též se nazývá testování metodou glass box a strukturální testování.

2.23 **Role pro přístup, specifický soubor oprávnění k přístupu,** např. uživatel, správce apod.

3. Interpretace článků normy ISO/IEC 17025 týkajících se počítačů a softwaru

V normě ISO/IEC 17025 existuje více článků, které mohou souviset se softwarem a/nebo s počítači. V níže uvedené tabulce je přehled těch článků, které by mohly být implementovány s použitím počítačových systémů.

Tabulka 1: Počítače a software v normě ISO/IEC 17025

Článek v ISO/IEC 17025	Je v článku přímá zmínka o počítači, softwaru nebo IT?	Interpretace a poznámky
4.1.5 c)	ano	Jestliže se počítače používají ke shromažďování informací zákazníka, musí být zabezpečeny (např. přístupem prostřednictvím login ID a role pro přístup)
4.1.6	ne	Za vhodný proces komunikace se považuje elektronická komunikace, např. e-mail, intranetové stránky apod.
4.2.7	ne	Lze aplikovat i na elektronické systémy managementu.
4.3.1	ne	Vztahuje se na dokumenty, zprávy apod. v elektronickém formátu.
4.3.2.1*	ne	Bez požadavků na elektronický podpis, pouze schválení např. prostřednictvím systému řízení znalostí a zápisového přístupu do adresáře.
4.3.2.2*	ne	Nelze aplikovat, jelikož na intranetu existuje jen jeden exemplář. Disclaimer – s odkazem na nekontrolovaný tisk nebo tisk řízený uživatelem.
4.3.3.2*	ne	Mohou být použity změny stopy nebo některá manuální metoda, je-li požadováno.
4.3.3.4*	ano	Způsob jak udržovat dokumenty, referenční systém řízení znalostí apod.
4.4.1 a)	ne	Laboratoř má deklarovat stupeň zabezpečení svého elektronického přenosu, jak zkušebních zpráv, tak v určitých případech i korespondence.
4.6.1	ne	Lze aplikovat i na software a počítače, viz též článek 5.5.2.
4.6.2	ne	Lze aplikovat i na software a počítače, viz též článek 5.5.2.
4.6.3	ne	Lze aplikovat i na software a počítače, viz též článek 5.5.2.
4.13.1.2	ne	Je třeba zajistit, aby byl po celou dobu uchovávání čitelný formát záznamů o kvalitě a technických záznamů. Migrace dat je nezbytná.
4.13.1.3	ne	Lze aplikovat i na elektronické záznamy.
4.13.1.4 (5.4.7.2 b))	ano	Je třeba zajistit, aby existovaly postupy pro zálohování a pro ochranu proti neoprávněnému přístupu k elektronickým záznamům.
4.13.2.1	ne	Zpravidla není nutné, aby byl starý počítačový systém udržován po celou dobu uchovávání záznamů, je však nezbytná schopnost podat na základě validace důkaz o přijatelnosti systému v době použití.
4.13.2.2	ne	Identifikace dat ve vztahu k pracovním úkolům.

Článek v ISO/IEC 17025	Je v článku přímá zmínka o počítači, softwaru nebo IT?	Interpretace a poznámky
4.13.2.3	ano	Je třeba, aby laboratoře identifikovaly pracovní relaci u počítače, a aby u změn dat mimo relaci byly nutné prověřovací záznamy (tj. data nejsou vymazána, nýbrž přestávají platit).
5.4.1	ne	Tento článek zahrnuje uživatelskou příručku softwaru.
5.4.7.1	ne	Během validace softwaru se ověřují automatizované výpočty a přenosy dat. Další kontroly nejsou zapotřebí, dokud nedojde k iniciaci revalidace.
5.4.7.2 a)	ano	Mimo to u koupeného softwaru je jako kontrola podle článku 5.5.2 nutný akceptační test.
5.4.7.2 b)	ne	Viz článek 4.12.1.4. Zabezpečení při přenosu dat je třeba brát v úvahu např. při přezkoumávání smlouvy. Je třeba pamatovat na ochranu proti virům apod.
5.4.7.2 c)	ano	Neliší se od jakéhokoli jiného zkušebního zařízení.
5.5.2	ano	Software/mikroprogramové prostředky splňují požadavky uživatele prostřednictvím akceptačních testů nebo validace.
5.5.4	ano	Každá instance softwaru má být podrobena akceptačním testům ve svém počítačovém prostředí.
5.5.5	ano	Software je třeba považovat za specifickou část zkušebního zařízení. Doklad o validaci a/nebo ověření je třeba udržovat obdobně jako u kalibrace.
5.9.2	ne	Data o řízení kvality mohou být shromažďována a/nebo analyzována počítačem a softwarem.
5.5.10	ne	Nutné jsou pravidelné kontroly, zda se u objektů softwaru nezměnil rozměr nebo časový údaj. Změny zavedeného systému iniciují revalidaci.
5.5.11	ano	Kontrola je nutná pouze při manuální činnosti. Při automatickém shromažďování dat pomocí validovaného softwaru není zapotřebí.
5.5.12	ano	Existuje-li role správce dovolující přístup ke všem dostupným funkcím, neměla by být při provozní činnosti využívána. Vhodnější je omezenější role pro přístup uživatele při provozní činnosti.
5.10.1	ano	Zprávy posílané zákazníkům v elektronické podobě nesmí být možno editovat. Je třeba používat zprávy v blokovaném formátu (např. jako soubor typu pdf).
5.10.2 j)	ne	Elektronické vyhotovování prvotních zpráv musí být v souladu s národními právními předpisy, které se vztahují na elektronický podpis, např. podpis PKI. V ostatních případech je výhodnější připojit ke zprávě naskenovanou celou stránku s podpisem.
5.10.7	ano	Elektronický přenos musí být zašifrován, není-li při přezkoumání smlouvy dohodnuto jinak.

* Poznámky k těmto článkům se týkají stavu, kdy příručka kvality je uložena pouze v elektronické podobě, např. jako dokument Wordu na síťovém disku s ochranou proti zápisu.

4. Různé kategorie softwaru

V tabulce 2 jsou různé typy softwaru roztříděny do pěti odlišných kategorií. Tabulka obsahuje příklady skupin programů i příklady specifických programů. Existují též jiné způsoby roztřídění softwaru, např. COTS (commercial off-the-shelf – volně prodejný software), MOTS (modified off-the-shelf – modifikovaný volně prodejný software) a CUSTOM (zakázkový software) [6]; tyto kategorie jsou v tabulce rovněž uvedeny.

Tabulka 2: Různé kategorie softwaru

Kategorie	Typy	Skupiny programů, příklady	Příklady programů
1 (COTS)	Operační systémy (COTS*)	Operační systémy	Windows, LINUX
2 (COTS)	Mikroprogramové prostředky (COTS)	Embedded software, vestavěný software	Přístroje, voltmetry, trhací stroje
3 (COTS)	Standardní sady programů, volně prodejný software (COTS)	e-mailové programy, textové editory	Word, Excel (pouze jako tabulka), Outlook, Internet Explorer, Acrobat, sériový software pro řízení přístrojů používaný vně přístroje
4 (MOTS)	Sady konfigurovaných programů (MOTS, modifikovaný volně prodejný software)	Programy jako programovací a konfigurační prostředí. Před použitím musí být přizpůsobeny a upraveny.	Vzorce Excell, LabView, Lab Windows, Labtech Notebook, Mathcad
5 (CUSTOM)	Zakázkový software (CUSTOM)	Software sestavený na zakázku pomocí programovacích nástrojů. Zahrnuje dokumenty Word/Excel s kódem makroinstrukce (kód VBA)	Aplikace sestavené v jazyku C++, SQL+, Java Visual Basic, XML, LabView, Lab Windows a jiných jazycích. V některých případech mohou být za zakázkové považovány aplikace.

5. Hodnocení rizika včetně zabezpečení

O riziku spojeném se zaváděním a používáním počítačů, počítačových systémů a softwaru v laboratořích se norma ISO/IEC 17025 výslovně nezmiňuje. Avšak úroveň rizika má vliv na rozsah a obsah procesu validace, a proto se o něm v těchto pokynech stručně pojednává. Tato kapitola podává pouze přehled tohoto námětu, četné příklady analýzy rizika jsou v literatuře.

Před zavedením nového softwaru, počítačů, zařízení obsahujících počítače apod. je třeba vyhodnotit riziko, které je s jejich zavedením spojeno. Účelem hodnocení rizika je určit rozsah a obsah potřebné validace a/nebo ověření. Toto hodnocení může zahrnovat, mimo jiné:

1) identifikaci možných událostí, které mohou vést k neshodě se zřetelem k normě ISO/IEC 17025 (např. k nesprávným výsledkům);
2) odhad pravděpodobnosti těchto událostí;
3) identifikaci následků těchto událostí;
4) způsoby, jak těmto událostem zabránit (např. použitím kontrolních etalonů/standardů nebo referenčních materiálů při kalibraci/zkoušení);
5) náklady, nevýhody, přínosy apod. spojené se zvolenými způsoby podle 4);
6) analýzu důsledků vyplývajících z bodu 5) ve spojení s bodem 3);
7) rozhodnutí o činnostech;
8) kancelářský nebo zkušební software.

V laboratoři jsou rizika v mnoha případech spojena s výsledky zkoušek a kalibrace a s využitím těchto výsledků.

Výsledek hodnocení rizika se používá ke stanovení rozsahu validace softwaru i zkušebních a kalibračních metod.

V normě ISO/IEC 17025 je jen několik článků, které od laboratoří výslovně požadují, aby měly postupy apod. pro zabezpečení počítačů a IT. Jsou to články 4.13.1.4, 5.4.7.2 b) a 5.10.7 uvedené v tabulce 1. Mnohé laboratoře však potřebují širší návod v těchto záležitostech, proto jsou v této kapitola obsaženy některé pokyny týkající se zabezpečení.

Tabulka v příloze 3 udává typická preventivní opatření předpokládaná pro různé stupně požadavků na zabezpečení. Připomeňme, že pojem „zabezpečení“ v tomto kontextu zahrnuje otázky integrity/přesnosti.

V tabulce v příloze 3 se integrita (hlavně požadavky na přesnost dat) a dostupnost považují za různé otázky. Preventivní opatření jsou rozdělena do skupin podle „požadavků“; s tím, jak se požadavky na zabezpečení stupňují od nízkých k vysokým, se přísnost opatření, která se zde považují za vhodná, zvyšuje. „Příklady“ uvedené v jednotlivých částech naznačují scénáře, které lze v každé z těchto částí předpokládat.

Ve většině případů v závislosti na stupni požadavků lze riziko řídit buď přijímáním podstatně přísnějších postupů, nebo přijímáním kombinací opatření. Například kombinace fyzického řízení přístupu a běžné ochrany heslem může být v praxi sejně účinná jako biometrická identifikace s méně přísnými fyzickými opatřeními k řízení přístupu.

Různá opatření mohou mít větší nebo menší důležitost v závislosti na individuálních okolnostech. Například velmi krátké termíny pro předání zprávy mohou u zkušební laboratoře vynucovat mnohem vyšší stupeň redundance hardwaru a pohotovosti oprav a údržby, než by vyplývalo z kritičnosti samotných dat.

Jestliže mají systémy IT rozhodující význam pro podnikání, je třeba zabránit neoprávněným změnám řízením přístupu (např. ochranou heslem nebo fyzickým zabezpečením přístupu). Pokud nejsou kritické systémy tímto způsobem chráněny, doporučuje se uživatelům, aby před použitím systému potvrdili a dokumentovali stav konfigurace.

A konečně je nanejvýše důležité, aby si všichni pracovníci byli vědomi, že existují vhodné postupy a musí být dodržovány. Při příchodu nových pracovníků a/nebo při školení personálu je nutné, aby každá osoba byla seznámena s otázkami zabezpečení IT a příslušně zaškolena. Je třeba, aby si pracovníci uvědomovali své povinnosti.

Požadovaný stupeň zabezpečení při elektronickém hlášení výsledků zkoušek a kalibrace je třeba dohodnout se zákazníkem v rámci přezkoumávání smlouvy. Integrita a důvěrnost závisejí na smluvní dohodě. Zabezpečení je v praxi závislé na dojednané smlouvě nebo se řeší v rámci přezkoumání smlouvy.

6. Ověřování a validace softwaru

Ověřování/validace softwaru závisí na tom, zda je software zakoupený nebo sestavený na zakázku. Potřebný rozsah této činnosti by měl vycházet z hodnocení rizika. Koupený software je třeba zkontrolovat (ověřit) k potvrzení jeho použitelnosti v prostředí uživatele. Typickým příkladem toho jsou akceptační testy srovnáváním se specifikacemi výrobců a/nebo požadavků uživatele.

Zakázkový nebo modifikovaný software musí být v potřebném rozsahu validován. Návod poskytuje tabulka 3.

Tabulka 3: Testování a validace softwaru

Kategorie softwaru	Riziko IT		
	nízké	**střední**	**vysoké**
Kategorie 1 Operační systémy (COTS)	Operační systémy samy se netestují. V případě zdokonalení operačních systémů je při středním/vysokém riziku nutný nový akceptační test softwaru v kategorii 4-5.		
Kategorie 2 Mikroprogramové prostředky (COTS)	Bez validace	Software je součástí zařízení, které musí být testováno/ kalibrováno podle normy ISO/IEC 17025 článku 5.5.2. V tom může být zahrnuta např. validace V1, V4 a testy T1, v závislosti na dotyčném zařízení.	
Kategorie 3 Standardní sady programů (COTS – volně prodejný software)	Bez validace	Kontrola vstupu/výstupu z hlediska konzistence (např. vzájemné hodnocení dokumentů). Příklad: textový editor používaný k psaní zkušebních zpráv.	Validace V1, V4 Testy T1-T2
Kategorie 4 Sady konfigurovaných programů (MOTS)	Kontrola vstupu/výstupu z hlediska konzistence (např. vzájemné hodnocení dokumentů).	Validace V1, V4 Testy T1-T3	Validace V1-V5 Testy T1-T4
Kategorie 5 Zakázkový software (CUSTOM)	Validace V1, V4 Testy T1	Validace V1-V5 Testy T1-T3	Validace V1-V5 Testy T1-T5

Fáze validace V1-V6 představují jednotlivé fáze typického plánu validace založeného na životním cyklu softwaru, jak ukazuje níže uvedená tabulka. Plán validace v rámci životního cyklu zahrnuje validaci a proces vývoje softwaru. Organizace, která software vyvíjí, je odpovědná za fáze V2 a V3 a koncový uživatel odpovídá za hlavní část fází V1, V4 a V5.

Tabulka 4a: Fáze validace

V0	Dokumentace výrobců
V1	Specifikace požadavků
V2	Návrh a zavedení (kódování)
V3	Kontrola a strukturální testování (testování metodou white box)
V4	Instalace
V5	Akceptační test (testování metodou black box)
V6	Provoz a údržba (v textu)

Různé typy testů metodou black box (T1-T6) uvedené v tabulce 3 jsou specifikovány v tabulce 4b.Tabulka zahrnuje příklady typických testů metodou black box používaných při validaci softwaru, uvedený přehled ovšem není vyčerpávající.

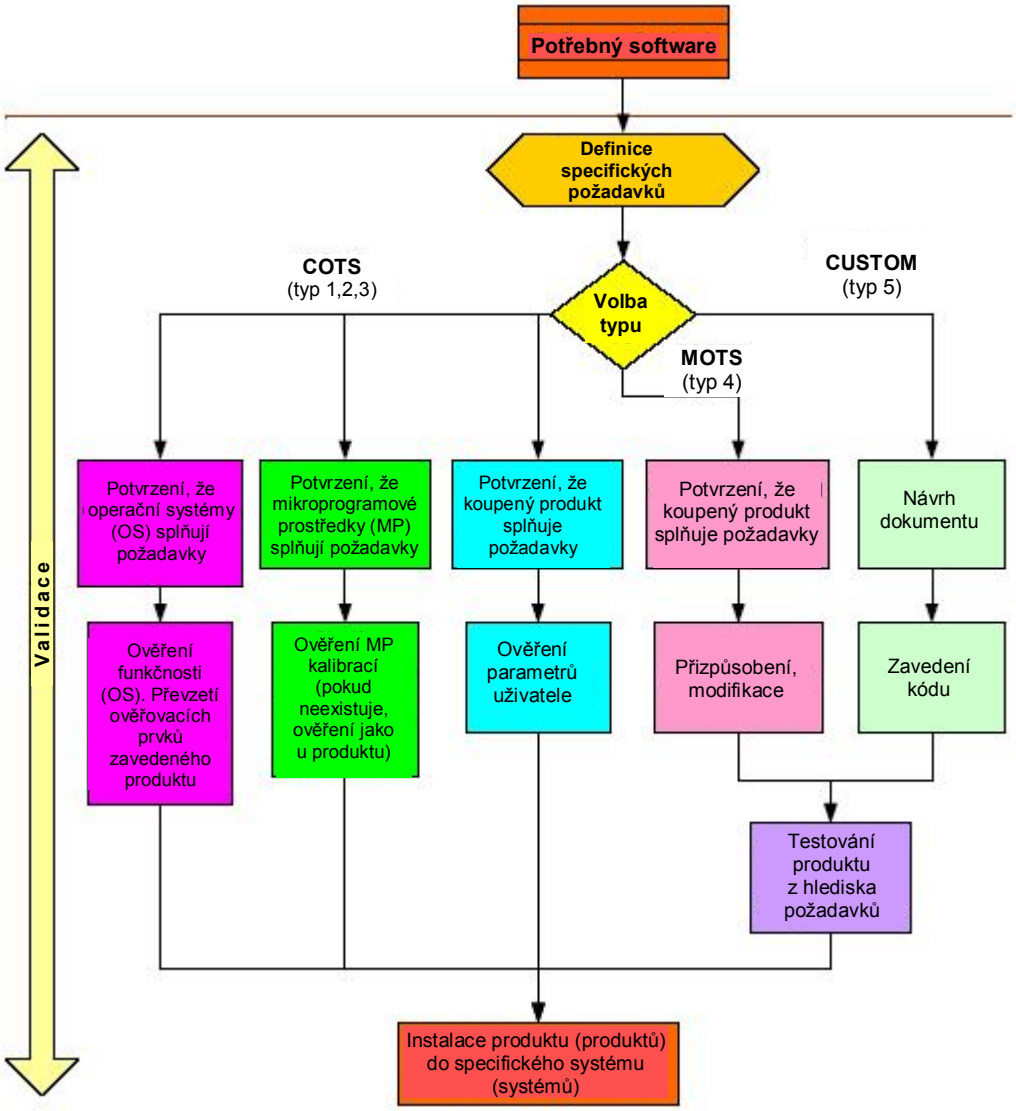
Tabulka 4b: Testy metodou black box

T0	Dokumentace výrobců
T1a	Typický soubor vstupních dat, kontrola zřetelných vad v produkovaném výstupu.
T1b	Test přenosu dat přímým pozorování, např. z přístroje do datového souboru za typických pracovních podmínek.
T2	Test funkčnosti softwaru, zejména z hlediska integrity, návaznosti, oprávnění k přístupu, zabezpečení apod.
T3a	Soubor typických vstupních dat, kde se produkovaný výstup kontroluje srovnáváním s „paralelním“ zpracováním dat (např. s manuálním výpočtem, s referenčním softwarem).
T3b	Kalibrace „známých“ etalonů/standardů (např. s historií nebo vzájemným porovnáním).
T3c	Generování souboru typických zkušebních dat se známým výstupem výsledku.
T4a	Generování souboru dat pro analýzu okrajových hodnot.
T4b	Generování souboru dat s neočekávanými hodnotami (extrémní vstupní data).
T4c	Test přenosu dat za extrémních podmínek, např. při stresových situacích přístrojů nebo softwaru.
T5	Testování se simulací jednotlivých zařízení.

Podle normy ISO/IEC 17025 článku 5.4.7.2 musí být validován veškerý software, který se používá ke kalibraci nebo zpracování zkušebních dat, s výjimkou softwaru v kategoriích 1-3 podle tabulky 2, kde je „validace“ omezena na akceptační test. Avšak veškerý software používaný při zkouškách nebo kalibraci musí být schopen dosáhnout požadované přesnosti a odpovídat příslušným specifikacím. Proto musí být provedeny fáze validace V1 a V4 i u softwaru kategorie 3. Úroveň validace závisí na typu softwaru a jeho aplikaci. Součástí validace softwarového produktu v laboratoři mohou být i jiné zprávy o validaci, jakož i veškerá historie bezporuchového provozu.

Podrobněji se o výše uvedené validaci a/nebo postupech validace pojednává v [7].

Na obrázku 1 jsou znázorněny různé cesty zavádění nového nebo upraveného softwaru v laboratoři, v závislosti na kategorii softwaru. Je zřejmé, že nové verze softwaru musí být před zavedením v laboratoři zkontrolovány/validovány. Rozsah validace závisí na softwaru a jeho použití, jakož i na riziku, které je s jeho používáním spojeno.



Obrázek 1: Různé cesty zavádění nového softwaru v laboratoři

Článek 5.4.7.2 a) normy ISO/IEC 17025 nelze interpretovat tak, že je přípustné použití softwaru bez jakékoli kontroly/validace, pokud byl vyvinut jinou organizací než laboratoří. Podle článku 5.5.5 je zřejmé, že u takového softwaru je třeba před jeho uplatněním v každodenní činnosti provést určitý druh kontroly/validace/akceptačního testu. Hlavní odpovědnost za kontrolu/validaci a za způsob jejího provedení může být předmětem smluvní dohody mezi organizací, která software vyvinula, a laboratoří. Laboratoř však nese hlavní odpovědnost za stav zařízení (včetně softwaru).

Ke splnění tohoto požadavku je nutná určitá přejímka ze strany uživatele nebo akceptační test. Převzaté zakázkové systémy („custom legacy systems“) lze považovat za koupený software pouze do doby, kdy vyžadují modifikaci. V tomto okamžiku se opět mění na zakázkové a vyžadují validaci.

Je velice důležité, aby veškeré validace, změny, verze a klíčová porovnání byly souběžně dokumentovány. Je nutné, aby byly dokumentovány změny provedené u IT hardwaru a softwaru, včetně aplikačních programů (např. v místním provozním deníku).

Tyto informace mohou zahrnovat údaje o tom, kdo změny provedl nebo schválil, datum a důvod, včetně testů provedených k potvrzení správné funkce.

Četné laboratoře používají ve své každodenní činnosti tabulkové kalkulátory, např. excel. V závislosti na rozsahu programování by měly být validovány jako software kategorie 3 (COTS) nebo kategorie 4 (MOTS). K úpravě tabulkových kalkulátorů směřují tyto pokyny:

- používejte zbarvení nebo stínování kolonek k odlišení jejich charakteru,
- zablokujte kolonky, které nejsou určeny pro vstupní data,
- chraňte tabulky tabulkového kalkulátoru a pracovní záznamy heslem,
- vložte instrukce pro operátory do tabulkového kalkulátoru, který přijímá vstupní data, nebo do jejich vlastních kalkulátorů,
- nastavte formát kolonek tak, aby byl vhodný pro data, která se mají do nich vložit.

Pokud je to vhodné, mohou být kontrolovány/testovány tyto parametry tabulkového kalkulátoru:

- správnost implementace výpočtů,
- správnost zkopírování opakovaných výpočtů,
- zaokrouhlování na správném místě ve výpočtu,
- přesnost výpočtů s použitím standardních nebo referenčních testovacích dat,
- správné zacházení s parametry s použitím testovacích dat s hodnotami parametrů uvnitř, na okraji a vně rozsahu přípustných/očekávaných hodnot.

7. Elektronické dokumenty, jejich zpracování, přenos a archivace

O některých otázkách týkajících se elektronických dokumentů již byla zmínka v tabulce 1. Obecně lze konstatovat, že by neměl být větší rozdíl v požadavcích kladených na laboratoře, které používají elektronické dokumenty, a laboratoře používající dokumenty tištěné na papíře. Nesmí se však zapomínat, že zavádění elektronických dokumentů se nabízí jak pro speciální příležitosti, tak pro specifické problémy, přičemž v normě ISO/IEC 17025 je několik článků, kde se o zpracování, přenosu a archivaci elektronických dokumentů hovoří. V článku 4.13 „Řízení záznamů“ je několik odstavců, které mají pro uživatele elektronických dokumentů specifický význam. Pojednává se zde například o nutnosti zálohování, o prověřovacích záznamech*, o chybách v záznamech a o uchovávání záznamů. Tyto odstavce jsou však jasné a právě tak jako u tabulky 1 by neměl být problém s jejich interpretací.

V normě je velmi málo požadavků týkajících se platných podpisů dokumentů. Jedním příkladem je článek 4.13.2.3, kde je požadavek, aby změny v záznamech byly podepsány nebo parafovány. Rovněž je užitečné, aby změny byly datovány. V elektronických dokumentech to lze řešit oprávněním k přístupu a zřetelným označením změny poznámkou, kdo změnu provedl. Tento způsob se nazývá prověřovací záznam a je elektronickou verzí tradičního způsobu škrtání, parafování a datování používaného ve světě tištěných dokumentů.

Požadavek týkající se podpisů nebo ekvivalentní identifikace je též v článku 5.10.2 „Protokoly o zkouškách** a kalibrační listy“.

Tento požadavek může být splněn „pravým“ elektronickým podpisem pomocí standardní technologie PKI (public key infrastructure) (což je dobrým řešením u zpráv/certifikátů, které mají právní konsekvence) nebo naskenováním stránky s „inkoustovým“ podpisem a jejím uložením v bezpečně uzamčeném formátu, např. pdf.

Elektronický přenos zkušebních zpráv a kalibračních listů má být zašifrován, není-li ve smlouvě nebo v přezkoumání smlouvy dohodnuto jinak. V běžné elektronické komunikaci se zákazníky bývají vzácné případy, kdy hrozí informacím zvýšené riziko, aby neskončily ve špatných rukách. Při normálních laboratorních činnostech to není pravděpodobné a vůči reálnému riziku by měla být přijata přiměřená opatření k zabezpečení.

Při uchovávání a archivaci elektronických dokumentů je třeba učinit opatření, která zajistí jejich vyhledání po celou dobu jejich uchovávání. K používaným metodám by měla patřit migrace do nových médií a/nebo opětné uložení do nových budoucích formátů.

---

* „Prověřovací záznam“, anglicky „audit-trail“; v české verzi normy ISO/IEC 17025 je tento termín nesprávně přeložen jako „provádění auditů“ (poznámka překladatele).

** Podle normy ČSN EN 10204 (srpen 2005) se termín „test report“ překládá ekvivalentem „zkušební zpráva“ (poznámka překladatele).

8. Odkazy

[1] ISO/IEC 17025:2005 “General requirements for the competence of testing and calibration laboratories” (Všeobecné požadavky na způsobilost zkušebních a kalibračních laboratoří)

[2] IEEE Standard 610.12-1990 “IEEE Standard Glossary of Software Engineering Terminology – Description” (Významový slovník terminologie softwarového inženýrství – popis)

[3] ISO/IEC/IEA/IEEE 12207:1996 “Information Technology – Software Lifecycle Process” (Informační technologie – Procesy v životním cyklu softwaru)

[4] US FDA Guidance for Industry „Computerized systems used in clinical trials: 2001“ (Pokyny US FDA [americké Federální správy pro léky a potraviny] pro průmysl „Počítačové systémy používané při klinických pokusech“)

[5] Draft FDA Guidance for Industry “21CFR part 11: Electronic Records; Electronic Signatures Validation” (Návrh pokynů FDA pro průmysl: 21CFR část 11: Elektronické záznamy; validace elektronických podpisů), 2001

[6] Gregory D. Gogates, “Software Validation in Accredited Laboratories, A practical Guide” (Validace softwaru v akreditovaných laboratořích, praktické pokyny), Fasor, Lansdale Pennsylvania, 2001

[7] Carl Erik Torp, “Method of Software Validation” (Metoda validace softwaru), NT Technical Report 535, Nordtest, Helsinki, 2003

Další významné dokumenty:

* ISO/IEC 17799:2005 “Information technology – Security techniques – Code of practice for information security management” (Informační technologie – Bezpečnostní techniky – Soubor postupů pro management informační bezpečnosti)

* Návody GAMP, např. “The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture“ (Správná praxe automatizované výroby – Pokyny pro validaci automatizovaných systémů ve farmaceutické výrobě) – GAMP 4

* ISO/IEC 121119:1994 “Information Technology – Software Packages – Quality Requirements and Testing” (Informační technologie – Sady programů – Požadavky na kvalitu a její testování)

* Návody WELMEC, např. WELMEC 7.1, 2. vydání “Development of Software Requirements” (Vývoj požadavků na software) a WELMEC 7.2, 1. vydání “Software Guide” (Návod pro software)

* Measuring Instrument Directive 2004/22/EC (Směrnice Evropského parlamentu a Rady 2004/22/ES ze dne 31. března 2004 o měřidlech)

* Directive 95/46/EC Personal Privacy (Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob)

* ISO/IEC Technical Report 13233:1995 “Information Technology – Interpretation of Accreditation Requirements in ISO/IEC Guide 25 – Accreditation of Information Technology and Telecommunication Testing Laboratories for Software and protocol Testing Services” (Technická zpráva ISO/IEC 13233:1995, Informační technologie – Interpretace požadavků na akreditaci v ISO/IEC Pokynu 25 – Akreditace zkušebních laboratoří v oboru informační technologie a telekomunikací pro testování softwaru a protokolů)

* ADCM – Computer System Validation in Clinical Research – A Practical Guide (Validace počítačových systémů v klinickém výzkumu – Praktický návod) 2. vydání, 2004

Příloha 1

Zavedení IT

V tabulce A.1 jsou uvedeny příklady použití systémů IT v laboratořích akreditovaných podle normy ISO/IEC 17025. Účelem je zejména ukázat obecně rozsah implementace a praktické kontroly managementu, považovaný za vhodný pro různé stupně implementace IT. V určitém smyslu lze uvedené údaje též interpretovat jako riziko spojené se zaváděním IT.

Tabulka A.1: Použití počítačů a softwaru na různém stupni zavedení IT

Článek normy 17025	Požadavky na řízení pomocí IT			Poznámky
	nízké	střední	vysoké	
1-3				Není významné.
4.1 Organizace	Systémy tištěných dokumentů pro management a dokumentaci organizace; IT se užívá pouze k vyhotovování tištěných dokumentů k trvalému záznamu.	Záznamy jsou uchovávány a zpřístupňovány pomocí systémů IT, konečný záznam je však tištěný nebo je v tištěné formě vždy přístupný.	Záznamy jsou uchovávány pouze na systémech IT; přidělování oprávnění spočívá na aplikacích IT. Plánování do značné míry spočívá na aplikacích IT. Osobní údaje jsou uloženy na systémech IT.	Musí být určena osoba odpovědná za počítačový systém. Riziko je závislé na složitosti systému.
4.2 Systém managementu				Viz řízení dokumentů
4.3 Řízení dokumentů	Výlučný systém tištěných dokumentů. IT se užívá pouze k vyhotovování tištěných dokumentů.	Záznamy jsou uchovávány a zpřístupňovány pomocí systémů IT, konečný záznam je však tištěný nebo je v tištěné formě vždy přístupný.	Všestranný počítačový systém pro management dokumentace kvality, pověřování a řízení verzí.	Hlavním problémem je dostupnost. Je třeba sledovat přístup k elektronickým verzím. Viz články 4.3.2.2 a) a 5.4.1. Rovněž je důležité řízení přístupu k psaní dokumentů.
4.4 Přezkoumávání poptávek	Systém tištěných dokumentů, žádné elektronické kopie nebo jejich tvorba.	IT se užívá k ověřování informací, k vyhotovování tištěných dokumentů apod.	Elektronický přenos dokumentů v obchodně citlivých záležitostech, řešených se zákazníkem.	Obchodní tajemství vytváří významné riziko IT a obecně vyžaduje určitá preventivní zabezpečovací opatření i pro systémy textových editorů k udržení důvěrnosti.
4.5 Subdodávky	Pouze tištěné zprávy	Elektronické verze tištěných zpráv jsou důležité pro podávání zpráv zákazníkovi; přenos prvotních dat k dalšímu analyzování.	Prvotní data a/nebo zprávy se generují, přenášejí a automaticky užívají k vyhotovování zpráv přímo určených zákazníkovi.	Musí být dohodnut formát dat. Důležitá je kontrola neporušenosti dat. Obchodní tajemství zvyšuje požadavky na dohled nad utajením.
4.6 Nakupování služeb a dodávek	Nákup standardních PC pro administrativní účely.	IT se užívá k podávání zpráv o výsledcích měření; IT se užívá ke kontrole a získávání výsledků měření z jednotlivých přístrojů.	IT se obecně užívá k získávání, zpracování a předávání dat; systémy LIMS (laboratorní informační a manažerské systémy)	Akceptační test
4.6 Nakupované služby			Úroveň dohledu závisí na velikosti systému a na závislosti na subdodavateli.	Subdodavatelé IT musí podepsat prohlášení o utajení. Důležitá je dohoda o úrovni služby.
4.7 Služby zákazníkovi				Žádné

Článek normy 17025	Požadavky na řízení pomocí IT			Poznámky
	nízké	střední	vysoké	
4.8 Stížnosti (jako 4.11)	Systémy tištěných dokumentů; IT se užívá k vyhotovování tištěných dokumentů pro záznamy apod.			Může vzniknout problém s přístupem. Stížnost musí být řádně vyřízena.
4.9 Řízení neshodných prací při zkoušení	Systémy tištěných dokumentů; IT se užívá k vyhotovování tištěných dokumentů pro záznamy apod.	Systémy IT se užívají jako podpůrný prostředek k identifikaci podmínek vymykajících se kontrole. Záznamy se uchovávají v tištěné i elektronické podobě.	IT představuje jediný způsob identifikace nedostatků. Záznamy se uchovávají pouze na systémech IT.	
4.10 Zlepšování	Systémy tištěných dokumentů; IT se užívá k vyhotovování tištěných dokumentů pro záznamy apod.	Systémy IT ve větších organizacích přispívají k identifikaci možností zlepšení. IT se užívá jako podpůrný prostředek při rozhodování o zlepšení nebo při analýze dat pro získání informací.	Systém IT je jediným prostředkem k identifikaci možností zlepšení. IT se užívá k identifikaci vhodných opatření.	
4.11 Opatření k nápravě	Systémy tištěných dokumentů; IT se užívá k vyhotovování tištěných dokumentů pro záznamy apod. Systémy IT se nepříliš často a/nebo v malém rozsahu užívají ke sledování nápravných opatření.	Systémy IT přispívají ke sledování nápravných opatření v rámci větších organizací. IT se užívá jako podpůrný prostředek při rozhodování o nápravných opatřeních nebo při analýze dat pro získání informací.	Systém IT je jediným prostředkem ke sledování nápravných opatření. IT se užívá k identifikaci vhodných opatření.	
4.12 Preventivní opatření	Systémy tištěných dokumentů; IT se užívá k vyhotovování tištěných dokumentů pro záznamy apod.	Systémy IT přispívají k plánování preventivních opatření v rámci větších organizací. IT se ve značné míře užívá jako podpůrný prostředek při rozhodování o preventivních opatřeních nebo při analýze dat pro získání informací.	Systémy IT jsou jediným prostředkem k řízení záznamů, ke sledování nedostatků apod. Přezkoumávání systému managementu spočívá výhradně na IT.	
4.13 Řízení záznamů				Viz řízení dokumentů
4.14 Interní audity		Plánování	Plánování	
4.15 Přezkoumávání systému managementu	Na systémech IT se uchovávají necitlivé informace (nikoli osobní údaje nebo obchodně citlivé údaje) a užívají k přezkoumávání.	Některé citlivé informace se uchovávají na izolovaných systémech IT; významná závislost na statistických informacích získávaných pomocí IT.	Přezkoumávání systému managementu spočívá výhradně na informací založených na IT. [Vzácné případy]	Manažeři se při přezkoumávání systému managementu zřídka spoléhají pouze na IT.
5.1 Všeobecné technické požadavky				Žádné

Článek normy 17025	Požadavky na řízení pomocí IT			Poznámky
	nízké	střední	vysoké	
5.2 Osoby pracující v laboratoři	Netýká se.	Systémy IT se užívají k vyhotovování tištěných záznamů.	Systémy IT se užívají k uchovávání všech osobních údajů, jako je mzda, kontaktní údaje, zdravotní informace.	i) Používání IT k vedení osobních záznamů bývá vázáno požadavky národních právních předpisů týkajících se používání osobních údajů. Požadavky právních předpisů musí být splněny. ii) U osobních záznamů je pravděpodobně nejdůležitější záležitostí řízení přístupu k zachování důvěrnosti. Důležitá je též integrita (k zabránění nesprávnému zacházení s údaji), tu však lze zpravidla pravidelně kontrolovat s dotyčnými osobami.
5.3 Prostory a podmínky prostředí	Netýká se	IT monitoruje prostředí a poskytuje informace pro rozhodování o regulaci prostředí.	IT se užívá k regulaci laboratorního prostředí v kritických oblastech (např. teploty nebo vlhkosti v klimatizovaných oblastech, zkušebních komorách apod.).	
5.4 Zkušební metody a validace metod	Netýká se	Systémy IT se užívají k vyhotovování tištěných kopií zkušebních metod. Systémy IT se užívají k provádění výpočtů používaných při validaci.	Zkušební metody pouze na systémech IT (LIMS).	Je třeba zajistit, aby řízení elektronických dokumentů poskytovalo „snadno přístupné“ metody.
5.5 Zařízení	Elektronický systém provádí pouze jednoduché operace řízené operátorem a produkuje prvotní data pro další zpracování.	Systém IT se užívá k řízení jednotlivých přístrojů nebo přístrojů velmi podobného typu; systém IT zpracovává data a generuje výsledky pro pozdější vypracování zprávy. Dohled vykonávaný zkušeným operátorem. Kontrola konfigurace.	Systém IT řídí několik zařízení nebo sbírá a/nebo zpracovává data z několika zařízení různého typu. Zařízení pracují výhradně s řízením IT a výstupy jsou generovány pod minimálním dohledem operátora. Kontrola konfigurace.	Systémy IT „významné“ pro zkoušení se považují za zařízení a před uvedením v činnost musí být validovány nebo ověřeny.
5.6 Návaznost měření	Kalibrační údaje se neuchovávají na systémech IT. Kalibrační údaje se vkládají z tištěných záznamů k podpoře získaných výsledků na základě jednoduchých výpočtů.	Ve složitých výpočtech na bázi IT se užívají kalibrační údaje z různých zdrojů, včetně tištěných. Podléhá dohledu operátora.	Kalibrační údaje se uchovávají výhradně na systémech IT a automaticky se používají při získávání výsledků a uvádění informací o návaznosti ve zprávách.	
5.7 Vzorkování	Systémy IT se nepoužívají nebo užívají k tvorbě tištěných plánů vzorkování a tištěných záznamů.	Systémy IT se užívají při plánování vzorkování s použitím geografických nebo jiných dat IT užívaných při automatickém zaznamenávání informací o vzorkování (času, polohy apod.).	Systémy IT řídí fyzické vzorkování a poskytují všechny příslušné záznamy.	

Článek normy 17025	Požadavky na řízení pomocí IT			Poznámky
	nízké	střední	vysoké	
5.8 Zacházení se zkušebními položkami	Netýká se	Systémy IT se částečně užívají při manipulaci se vzorky nebo při jejich sledování (např. při označování, číslování apod.).	Veškerá manipulace se vzorky a jejich sledování spočívá na systémech IT (LIMS). Plně automatizované systémy manipulace se vzorky řízené vnější IT.	
5.9 Zajišťování kvality výsledků zkoušek				Žádné
5.10 Uvádění výsledků	Netýká se	IT se užívá k vyhotovování zpráv ke kontrole a podpisu.	IT elektronicky vyhotovuje zprávy. Rozsáhlé vyhotovování běžných tištěných zpráv.	

Příloha 2

Směrnice o měřidlech a používání sítí ve spojení s procesem měření

Tato příloha se opírá o výsledky projektu „software podle MID“, jehož předmětem je používání softwaru a IT u měřicích přístrojů, na které se vztahuje nová směrnice EU o měřidlech „Measuring Instruments Directive (MID)“*; projekt není součástí požadavků normy ISO/IEC 17025.

Rozložená síť měřicích systémů (přenos měřených dat ze vzdálených přístrojů, dálkově řízený provoz měřicích přístrojů)

a) **Uzavřená síť**

V případě uzavřených sítí není situace tak kritická.

b) **Otevřená síť**

U sítě s neznámými účastníky je nutné, aby příjemce jednoznačně identifikoval původ zprávy. Během přenosu může docházet k nepředvídanému zpoždění. Ke správnému přiřazení přijaté naměřené hodnoty k určitému měření musí být zaznamenána doba měření.

U každé naměřené hodnoty se tak předpokládá:

- identifikace měřicího přístroje,
- identifikace měření,
- časový údaj,
- označení zprávy (kontrolní součet [CRC], digitální označení hodnotou HASH nebo označení celé zprávy),
- zašifrování měřených dat (problematické, závisí na riziku).

Během vyhodnocování:

- ověření, zda software na straně vysílače provádí dané funkce,
- ověření, zda software na straně přijímače tyto funkce kontroluje.

Data detekovaná se známkami porušení nesmí být použita.

Klíče a doprovodná data (o nichž se pojednává i v jiných částech dokumentu):

Měření nesmí být nepřípustně ovlivňováno zpožďováním přenosu. K poruchám přenosu dochází náhodně a nelze je vyloučit. Vysílací zařízení musí být schopné tyto situace zvládnout. Reakce přístroje na stav, kdy přenos přestal fungovat, závisí na principu měření. Měření, která probíhají nepřetržitě, např. měření energie, objemu apod., nevyžadují zvláštní dočasnou vyrovnávací paměť, protože tato měření jsou vždy kumulativní. Data mohou být vyvolána z kumulativního registru a později po obnovení spojení přenesena.

Stahování softwaru (např. zjišťování chyb v programu, aktualizace, nové aplikace apod. u měřicích přístrojů)

Komunikační spoje mohou být přímé, např. RS 232, USB, v rámci uzavřené sítě s částečným nebo plným řízením, např. Ethernet, LAN Token Ring, nebo v rámci otevřené sítě, např. internet.

- Přístroj má být schopen zjistit poruchu při stahování nebo instalaci. Musí být vydána výstraha. Dojde-li k selhání nebo přerušení stahování nebo instalace, nesmí být ovlivněn původní stav měřicího přístroje. Alternativně musí přístroj ohlásit trvalou chybu a jeho metrologická funkce musí být zablokována, dokud nebude příčina chyby odstraněna.
- Během stahování a následující instalace staženého softwaru musí být měření zablokováno nebo musí být zaručena správnost měření.
- Počet pokusů o opětnou instalaci musí být omezený.
- Musí být k dispozici prostředky poskytující záruku, že stažený software je původní.

* Směrnice Evropského parlamentu a Rady 2004/22/ES ze dne 31. března 2004 o měřidlech (poznámka překladatele).

Před prvním použitím staženého softwaru musí měřicí přístroj automaticky ověřit, zda:

- software je autentický (nikoli falešná napodobenina),
- software je vyzkoušen pro daný typ měřicího přístroje.

Je nutné vhodnými technickými prostředky zaručit, že stažený legální software může být v rámci přístroje (systému) vysledován.

Je nutné technickými prostředky zaručit, že software může být zaveden pouze s výslovným souhlasem uživatele, popřípadě vlastníka měřicího přístroje.

Některé požadavky/doporučení týkající se hardwaru:

Přítomnost vady může nebo nemusí být zjevná. Ať již vada je nebo není zjevná, má závažnou poruchu detekovat samotný měřicí přístroj.

Příloha 3

Zabezpečení

V tabulce jsou uvedeny různé aspekty zabezpečení v souvislosti s používání IT v laboratořích.

Tabulka A.3

Předmět požadavků	Požadavky			Poznámky
	nízké	střední	vysoké	
Dostupnost				
Příklady:	Trvalá ztráta dat v systému IT není důležitá (např. vzhledem k existenci a spolehlivosti systému tištěných dokumentů). Dočasná nedostupnost v délce týdnů není kritická.	Trvalá ztráta dat způsobí vážnou ztrátu hodnověrnosti nebo si vyžádá značný objem dodatečné práce k opětnému vložení nebo obnovení dat. Nedostupnost systému po dobu 1-5 dní není kritická. Ztrátový čas 1-5 % není kritický.	Trvalá ztráta dat způsobí celkové selhání pracovního úkolu. Nedostupnost systému v řádu hodin nebo méně je kritická.	
Typická bezpečnostní opatření				
Uchovávání dat	Jediný paměťový systém (např. lokální pevný disk) s původním softwarem uchovávaným pro obnovování.	Jediný hlavní paměťový systém (pevný disk, síťový server)	Vícenásobné redundantní paměťové systémy (zrcadlové disky, RAID apod.). Paměť „hot-swappable“	Požadavky na zálohování závisejí na přijatelném časovém měřítku ztrát (např. jestliže ztráta polodenní práce může být kritická, musí se zálohovat nejméně dvakrát denně).
Obnova	Zálohování podle uvážení uživatele (např. během přípravy zprávy, kdy ztráta dat by mohla zpozdit její vydání).	Vhodný je systém zálohování jednou denně až týdně (doporučuje se hierarchický zálohovací systém). Ukládání dílčích záložních kopií na bezpečném/ ohnivzdorném místě. Data se ukládají nejméně jednou týdně mimo pracoviště.	Plně automatizované přírůstkové zálohování během hodin. Přímé dálkové zálohování. Bezpečné ukládání mimo pracoviště	
Migrace dat		Autorizovaný software pro ukládání dat může způsobovat potíže při migraci dat.		
Zálohovací média	Magnetická média	Magnetická média s vhodnou dobou existence uchovávaná za vhodných podmínek skladování. Magnetooptická média		Média závisejí na požadované době skladování.
Redundance hardwaru	Žádná	*Buď*: Záložní systém určený pro nouzové použití (např. druhý PC nebo server, který může být dočasně přizpůsoben jako náhrada), *nebo*: přijatá opatření pro rychlý pronájem/náhradu.	Vícenásobné redundantní systémy (např. rezervní souborový server s funkcí failover).	

Předmět požadavků	Požadavky			Poznámky
	nízké	střední	vysoké	
Údržba a opravy	Omezená záruka výrobce; zajištěna služba return-to-base.	Oprava na místě během 1 až 3 dnů.	Oprava na místě během čtyř hodin.	
Integrita				
Příklady:	Chyby v datech nejsou kritické. Numerická přesnost není kritická (např. stačí dvě platné číslice). Pozn.: V této kategorii nikdy nejsou měřená data u akreditované laboratoře.	Chyby v číselných hodnotách mají dopad na zákazníky. Chyby v ostatních datech mají významný dopad na zákazníka nebo jiné činnosti (např. předkládání chybných zpráv apod.). Postačuje běžná numerická přesnost (např. stačí 6-8 platných číslic). Pozn.: Do této kategorie spadá většina kalibračních a zkušebních dat.	Chyby mají kritický dopad z hlediska bezpečnosti nebo zdraví. Výsledky se užívají v trestním řízení. Důležitá je numerická přesnost na 8 platných číslic.	
Typická bezpečnostní opatření				
Ověřování/validace softwaru	Viz tabulka 3			
Řízení přístupu	Řízení přístupu má zajistit, aby uživatelé byli dostatečně seznámeni se systémy IT nebo aby instrukce byly snadno dostupné.	Řízením přístupu musí být zajištěno, aby pracovníci byli náležitě vyškoleni k používání systémů a měli potřebné dovednosti.		
Postupy	Zpravidla postačují nápovědné systémy pro systémy a software a/nebo manuály.	Nezbytné jsou nápovědné systémy pro systémy a software a/nebo manuály, které mají být podpořeny dokumentovanými instrukcemi (které mohou být elektronické) pro specifické výpočty/postupy, které využívají software.	Veškeré zavádění dat a výpočty musí dodržovat podrobně dokumentované postupy.	V každé akreditované laboratoři mají mít všechny systémy vhodné dokumentované postupy jejich používání.
Konfigurace softwaru	Software mohou instalovat schválení uživatelé.	Instalovaný software má být dokumentován (zpravidla postačuje změnový deník softwaru). Změny softwaru jakéhokoli druhu musí být řízeny a prováděny vhodně kvalifikovanými a zkušenými pracovníky, kteří jsou k tomu oprávněni.	Software by měl být instalován až po důkladném testování jeho kompatibility se systémem a dalším softwarem. Mají být zavedeny formální postupy pro autorizaci každé změny konfigurace	1. Musí být přijata opatření, která zabraňují náhodné nebo záměrné instalaci škodlivého softwaru. 2. Vždy musí být respektována licenční a autorská práva.
Stahování softwaru		Musí být přijata koncepce pro stahování a instalaci softwaru. Příklad: Windows 2000 Service Pack 4.		