Riskianalyysimenetelmät

Laajennettu tiivistelmä

Jouni Meriläinen
26. helmikuuta 2003
Helsingin yliopisto
Tietojenkäsittelytieteen laitos
Jouni.Merilainen@cs.helsinki.fi

Tiivistelmä

Kirjoituksessa tarkastellaan riskianalyysiä yleisesti ja kolmea lähestymistavaltaan erilaista, laajassa käytössä olevaa systemaattista riskianalyysimenetelmää erityisesti. Kohdealueena on tietoturva, mutta menetelmät soveltuvat hyvin tietojärjestelmien yleisempäänkin riskianalyysiin. Tarkasteltavat menetelmät ovat vika- ja vaikutusanalyysi (engl. FMEA), poikkeamatarkastelu (engl. HAZOP) ja vikapuuanalyysi (engl. FTA).

Johdanto

Riskillä tarkoitetaan yleiskielessä "jonkin menetyksen, tappion tai muun epäedullisen tapahtuman mahdollisuutta, uhkaa tai vaaraa". Riskien minimointia kutsutaan riskienhallinnaksi (engl. risk management). Sen ensimmäinen vaihe on riskianalyysi (engl. risk analysis), joka koostuu uhkien tunnistamisesta (engl. hazard identification) ja niiden riskien suuruuden arvioinnista (engl. risk estimation). Toinen vaihe on riskien merkityksen arviointi (engl. risk evaluation). Viimeinen vaihe, riskien valvonta (engl. risk control), pitää sisällään muun muassa toimet riskien pienentämiseksi. Terminologia ei ole täysin vakiintunutta.

Perinteinen riskianalyysi

Alkeellisimmassa riskianalyysin muodossa ei uhkien tunnistamiseen käytetä mitään järjestelmällistä menetelmää. Ongelmana on, että näin saatu uhkien luettelo ei välttämättä ole kattava. Oman mielikuvituksen avuksi voidaan ottaa esimerkiksi tarkistuslistat, kuten "toimialan 10 merkittävintä riskiä", tai riskitaksonomiat, joissa toimialan kaikki eri tyyppiset uhat on pyritty yleistämään ja luokittelemaan hierarkkiseksi järjestelmäksi. Voi myös laajentaa näkökulmiaan ja jäsentää ajatteluaan esimerkiksi laatimalla ensin erittelyn vaikkapa toiminnan tavoitteista (engl. goals) tai arvokkaista resursseista (engl. assets), ja miettiä sitten yksitellen näihin kohdistuvia uhkia. Uhkien välillisiä seurausvaikutuksia voi hahmottaa laatimalla uhkien toteutumisesta pieniä kertomuksia, skenaarioita.

Riskin suuruudella (engl. risk exposure) tarkoitetaan useimmiten menetyksen suuruuden odotusarvoa. Tämän määrittämiseksi riittää siis selvittää kunkin uhan todennäköisyys ja menetyksen suuruus uhan toteutuessa. Kumpikaan näistä osatehtävistä ei ole ongelmaton. Jotta menetyksiä voisi verrata keskenään, tarvitaan yhteinen mittayksikkö. Raha on määritelmänsä mukaan tällainen universaali arvon mitta, mutta sekään ei ongelmitta sovellu kaikkialle. Tuntuu varsin irvokkaalta mitata esimerkiksi ihmishengen menetystä rahassa. Menetyksen suuruuden määrityksessä on myös arkisempia pulmia. Voi olla vaikea ennakoida esimerkiksi menetetyn maineen tai kilpailijalle vuotaneen tiedon aiheuttamaa rahallista menetystä. Joissain

menetelmissä tyydytäänkin vain asettamaan mahdolliset menetykset vakavuus-järjestykseen keskenään tai jakamaan ne karkeasti vakavuusluokkiin.

Todennäköisyyden arviointikaan on harvoin helppoa. Todennäköisyyden frekvenssi-tulkintaa ei voida käyttää, jos tapahtuman esiintymistiheyttä vallitsevissa olosuhteissa ei tunneta. Ääritapauksessa voi arvioinnin kohteena olla tapahtuma, jota ei tiedetä ikinä tapahtuneen, mutta joka on selvästi mahdollinen. Usein joudutaankin turvautumaan subjektiivisen todennäköisyyden käsitteeseen eli mitataan omaa uskomuksen astetta — tehdään siis valistunut arvaus. Jälleen voidaan tyytyä arvioimaan todennäköisyysjärjestystä tai käyttämään karkeaa luokittelua.

Vika- ja vaikutusanalyysi (FMEA)

Vika- ja vaikutusanalyysi (engl. Failure Modes and Effects Analysis, FMEA) on luotettavuusanalyysimenetelmä, joka perustuu tutkittavan järjestelmän jakamiseen osajärjestelmiin ja lopulta osiinsa. Menetelmässä pyritään tunnistamaan kunkin osan eri vikaantumistavat (engl. failure mode) ja päättelemään niiden vaikutukset osa-järjestelmän ja lopulta järjestelmän toimintaan. Menetelmä on siis alhaalta ylös -tyyppinen (engl. bottom-up) eli induktiivinen. Lisäksi menetelmässä pyritään kartoittamaan, mikä on kunkin vikaantumistavan alkuperäinen syy (engl. root cause).

Riskien priorisointia varten arvioidaan haitallisen vaikutuksen vakavuutta asteikolla 1–10, missä kunkin luokan vakavuudella on sanallinen kuvaus. Vastaavasti vian esiintymistodennäköisyyttä arvioidaan asteikolla 1–10, missä kukin luokka vastaa tiettyä todennäköisyysväliä. Edelleen arvioidaan asteikolla 1–10, kuinka luultavaa on, että vika tai siihen johtavat syyt eivät paljastu ennen kuin niistä aiheutuu ongelmia, siis esimerkiksi järjestelmää testattaessa. Saadun kolmen luvun tulo on riskien merkityksen arvioinnin pohjana.

Menetelmän soveltuvuus suurelta osin ohjelmistoista koostuviin järjestelmiin ei ole yksiselitteinen. Ahtaasti tulkittuna ohjelmisto ei voi vikaantua — algoritmi on joko oikea tai väärä, mutta käytön aikana se ei vikaannu. Ohjelmiston toiminta on siis joka kerta samanlainen, jos syöte ja muut olosuhteet on mahdollista saada täsmälleen samoiksi. Toisaalta järjestelmissä voi kuitenkin olla piileviä tai harvoin esiintyviä virheitä, jotka ovat havaittavissa vain tietyissä olosuhteissa, joita ei tunneta. Jos vikaantumisen käsite tulkitaan riittävän laajasti, soveltuu vika- ja vaikutusanalyysi myös ohjelmistojen riskianalyysiin. Menetelmän hyviä puolia tietoturvan kannalta on, että riskin arvioinnissa otetaan huomioon, voiko vika olla olemassa niin, ettei sitä huomata. Näin siksi, että monissa tietoturvauhissa on tekijänä ilkeämielinen, salassa toimiva hyökkääjä.

Poikkeamatarkastelu (HAZOP)

Poikkeamatarkastelu (engl. Hazard and Operability study, HAZOP) on alunperin kemian teollisuuden käyttöön kehitetty menetelmä, jossa arvioidaan poikkeamien haitallisia vaikutuksia. Poikkeamia pyritään hahmottamaan seitsemän avainsanan avulla: *ei* tai *ei mitään, enemmän, vähemmän, lisäksi, osittain, päinvastoin, muu kuin.* Esimerkiksi avainsanan "enemmän" tapauksessa pohditaan, mitä jokin määrällinen lisäys voi aiheuttaa järjestelmässä, esimerkiksi oikeaa arvoa suurempi virtaus tai paine. HAZOP-menetelmä, kuten vika- ja vaikutusanalyysikin, on luonteeltaan alhaalta ylös -tyyppinen.

HAZOP-menetelmä on varsin helppo muuntaa tietojärjestelmän riskianalyysiin soveltuvaksi — tarvitsee vain samaistaa tietovuot virtausten kanssa. Myös tietoturvaan käsitteet sopivat hyvin. Useimmat tietoturvauhat on mallinnettavissa liittyviksi tiedon siirtymiseen.

Vikapuuanalyysi (FTA)

Vikapuuanalyysi (engl. Fault Tree Analysis, FTA) on edellisistä menetelmistä poiketen ylhäältä alas -tyyppinen (engl. top-down) eli deduktiivinen. Siinä pohdinta alkaa lopputuloksista, näkyvistä vioista, joita järjestelmässä voi esiintyä. Kukin näistä on oman puunsa juurisolmuna. Tämän jälkeen päätellään, minkä ehtojen voimassa ollessa vika voi esiintyä. Ehdot muodostavat puun seuraavan tason ja niitä yhdistää yleensä *ja*- tai *tai*-operaattori, tai harvemmin jokin muu looginen operaattori. Näiden ehtojen ehdot puolestaan muodostavat puun seuraavan tason ja niin edelleen, kunnes vikojen syyt on saatu analysoitua riittävällä tarkkuudella. Valmista puuta voi sieventää logiikan laskusäännöillä.

Kun puu on saatu muodostettua, liitetään sen lehtisolmuihin todennäköisyydet. Näistä lähtien on mahdollista laskea juurisolmun todennäköisyys käyttäen todennäköisyyslaskennan laskusääntöjä loogisille lausekkeille. Myös herkkyysanalyysi on hyödyllinen, jotta nähdään, mitkä lehtisolmut vaikuttavat eniten juurisolmun todennäköisyyteen.

Vikapuuanalyysi, kuten vika- ja vaikutusanalyysikin, soveltuu ohjelmistopohjaisten järjestelmien tutkimiseen, kunhan vian käsitettä ei rajata liian ahtaasti. Menetelmä vaikuttaa ensi katsomalta aukottoman varmatoimiselta. Sen tuottamien tulosten tarkkuutta rajoittavat kuitenkin niin lehtitason todennäköisyyksien tarkkuus kuin vikojen syiden mahdollisesti monimutkaiset keskinäiset riippuvuudetkin.

Kirjallisuutta

Johdanto

Haarala, R. et al. (toim.), *Suomen kielen perussanakirja, toinen osa L-R.* Kotimaisten kielten tutkimuskeskus, Helsinki, 1992.

Luotettavuusjohtaminen, osa 3: käyttöopas, luku 9: teknisten järjestelmien riskianalyysi. Standardi SFS-IEC 60300-3-9. Suomen standardisoimisliitto SFS ry, Helsinki, 2000.

Perinteinen riskianalyysi

Boehm, B.W., Software risk management: principles and practices. *IEEE Software* 8, 1 (January 1991), 32-41.

Carr, M. et al., *Taxonomy-based risk identification.* The Software Engineering Institute (SEI), Carnegie Mellon University, Technical Report CMU/SEI-93-TR-006, ESC-TR-93-183, Pittsburgh, PA, USA, 1993. `http://www.sei.cmu.edu/publications/documents/93.reports/93.tr.006.html` [24.2.2003]

Courtney, R.H. jr., Security risk assessment in electronic data processing systems. *AFIPS Conference Proceedings, National Computer Conference*, Dallas, TX, USA, June 13-16, 1977, 97-104.

Kontio, J., *The Riskit method for software risk management, version 1.00.* Institute for Advanced Computer Studies and Department of Computer Science, University of Maryland, Technical Report CS-

TR-3782, UMIACS-TR-97-38, College Park, MD, USA, 1997. http://soberit.hut.fi/~jkontio/riskittr.pdf [24.2.2003]

Parker, D.B., *Computer security management.* Reston Publishing Company, Reston, VA, USA, 1981.

Redmill, F., Exploring subjectivity in hazard analysis. *Engineering Management Journal* 12, 3 (June 2002), 139-144.

Tietoturvasanasto. Tekniikan sanastokeskus ry, Helsingin tietojenkäsittely-yhdistys ry, Helsinki, 1992.

Valtionhallinnon tietoturvallisuuskäsitteistö. Julkaisu VAHTI 1/2000, Valtiovarainministeriö, Helsinki, 2000. http://www.vn.fi/vm/kehittaminen/tietoturvallisuus/vahti/sanasto/sisallys.htm [25.2.2003]

Vika- ja vaikutusanalyysi (FMEA)

Haapanen, P., Helminen, A., *Failure mode and effects analysis of software-based automation systems.* Report STUK-YTO-TR 190, Säteilyturvakeskus, Helsinki, 2002. http://www.stuk.fi/julkaisut/tr/stuk-yto-tr190.html [25.2.2003]

Procedures for performing a Failure Mode, Effects, and Criticality Analysis. Military standard MIL-STD-1629A, Department of Defense, Washington, DC, USA, 1980.

Nguyen, D., Failure Modes and Effects Analysis for software reliability. *Proceedings Annual Reliability and Maintainability Symposium,* Philadelphia, PA, USA, January 22-25, 2001, 219-222.

Potential Failure Mode and Effects Analysis (FMEA) reference manual. Chrysler Corporation, Ford Motor Company, General Motors Corporation, 1995.

Poikkeamatarkastelu (HAZOP)

Bjuréus, P., Jantsch, A., MASCOT: A specification and cosimulation method integrating data and control flow. *Proceedings of the Conference on Design, Automation and Test in Europe,* March 27-30, 2000, 161-168.

Fenelon, P. et al., Towards integrated safety analysis and design. *ACM SIGAPP Applied Computing Review* 2, 1 (March 1994), 21-32.

Griffths, M.P., MASCOT 3. *IEE Tutorial Colloquium on Formal Methods and Notations Applicable to Telecommunications,* March 19, 1992, London, United Kingdom, 5/1-5/4.

McDermid, J.A., Pumfrey, D.J., A development of hazard analysis to aid software design. *COMPASS '94 Proceedings of the Ninth Annual Conference on Computer Assurance,* June 27 - July 1, 1994, Gaithersburg, MD, USA, 17-25.

McDermid, J.A. et al., Experience with the application of HAZOP to computer-based systems. *COMPASS '95 Proceedings of the Tenth Annual Conference on Computer Assurance,* June 25-29, 1995, Gaithersburg, MD, USA, 37-48.

Vikapuuanalyysi (FTA)

Briscoe, G.J., Risk management guide. United States Energy Research and Development Administration, ERDA 76-45/11, SSDC-11, UC-41, Washington, DC, USA, 1977.

Fault Tree Handbook. U.S. Nuclear Regulatory Commission, NUREG-0492, Washington, DC, USA, 1981. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/sr0492.pdf [24.2.2003]

Leveson, N.G., Harvey, P.R., Software Fault Tree Analysis. *The Journal of Systems and Software* 3, 2 (June 1983), 173-181.