STPA Software Module

A Eurostars Funded Project

5th European STAMP/STPA Workshop and Conference

13 - 15 September 2017 - Reykjavík, Iceland

Christopher Brown and Jianfei Zheng

Stiki Information Security

RM Studio Risk Management — Efficient and Effective

Microsoft Partner Gold Independent Software Vendor (ISV)

bsi. ISO/IEC 27001 Information Security Management BSI IS 67387

The Project Objectives

- Provide the STPA methodology in a structured software application
- Incorporate with a successful risk management software – Risk Management Studio®
- Operation as an independant analysis tool or in conjunction with traditional risk management

Stiki
Information Security

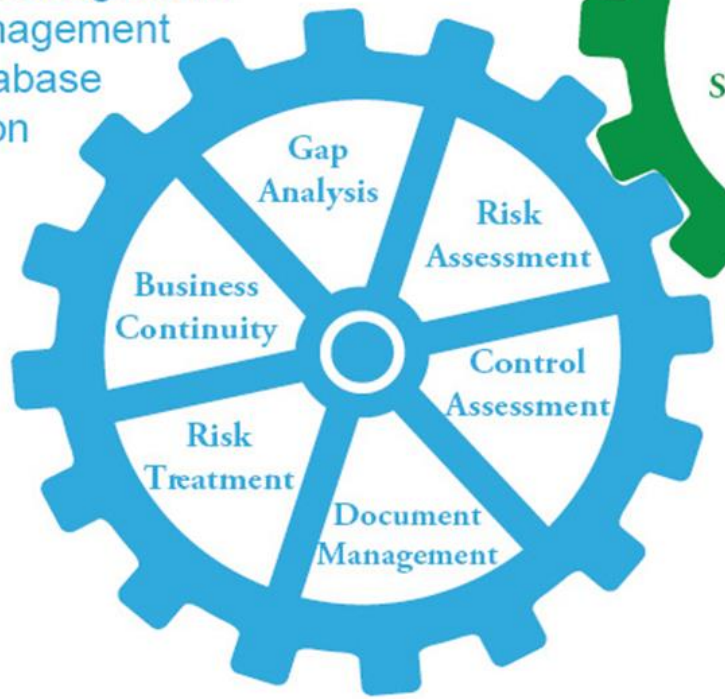
Objectives Visual Representation

RM Studio

The RM Studio features:

- Risk Management
- Document management
- Quality Management
- Central database
- Collaboration

and more



STPA

The STPA Module features:

- Hierarchical Control Structures
- UCA Assessment
- Control Loop Modelling
- Scenario Identification
- Report Generation

Stiki
Information Security

Principle Participants

- ❖ Stiki – Information Security, RM Studio®

- ❖ Safety-Critical Systems Research Lab of ZHAW,
  Zurich University of Applied Sciences

Additional support:

- Eurostars
- Technology Development Fund, Iceland
- Swiss Confederation, Federal Department of Economic Affairs, State Secretariat for Education, Research and Innovation SERI

Stiki
Information Security

Stiki's Story and Background

- 1992 — Founded: IT consulting solutions
- 2000 — Began work with RAI software Health Care Solutions
- 2002 — Internal Risk Assessment created for certification to ISO 9001 & ISO/IEC 17799
- 2005 — Stiki debuts RAI Suite: RAI Home Care, RAI Mental Health, RAI Post Acute Care
- 2006 — RM Studio v1 debuts: Risk Assessment & Risk Treatment for ISO/IEC 27001:2005
- 2009 — RM Studio v2 released 1st international sales in the U.K.
- 2011 — RM Studio v3 released Business Continuity Management
- 2013 — RM Studio v4 released Control Maturity Assessment
- 2015 — RM Studio v5 released Web module
- 2016 — STPA Application Project Begins
- 2018 — RM Studio STPA Module

Stiki Information Security

Svana's Research and Publications

2015 Comparison of Risk Analysis Methodologies – Risk Analysis for Better Design and Decision Making

4th STAMP Workshop at MIT, Boston, 23-26 March, ppt

2015 Comparison of Risk Analysis Methodologies in an Electrical Grid

3rd European STAMP Workshop, Amsterdam, 4-6 October, ppt

2016 Risk Analysis in Design and Construction of a Hydropower Station

4th European STAMP Workshop, Zürich, 13-15 September, ppt

2017 Embedding STPA into a Highly Successful Risk Management Software

6th STAMP Workshop at MIT, Boston, 23-26 March, ppt

Stiki Information Security

Zurich University of Applied Sciences

- 10 person team with broad backgrounds and work experiences
- Promotes technological progress and methodologies
  - Hazard and risk analysis
    - STPA
  - Functional safety of complex, programmable systems
  - Quantitative safety analyses
  - Formal specification, development and verification methods
- Responsibilities
  - Applied research and development projects
  - Teaching and consulting

Stiki
Information Security

Zurich University of Applied Sciences

2012 Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System

MIT PhD Dissertation by Blandine Antoine, Presentations at 1st MIT STAMP Workshop and 1st European STAMP Workshop 2013

2014 Use of STPA in Digital Instrumentation and Control Systems of Nuclear Power Plants

Presentations at 2nd European STAMP Workshop

2015 Tool Qualification Considerations for Tools Supporting STPA

Paper and Presentations at 3rd European STAMP Workshop

2016 Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management

Pharmaceutical Medicine, Springer and presentation at 4th ESW 2016

Stiki Information Security

Primary Project Challenges

Researching and choosing a diagraming tool that would perform the necessary actions required and be compatible with RM Studio

Deciding how to incorporate the STPA methodology into a working platform that will meet the needs of diverse industries

Colaboration between project contributors across multiple locations in Europe that satisfies many different business processes

Stiki
Information Security

STPA Module Infrastructure

- ✓Database
- ✓Diagraming high quality complex designs
- ✓Modeling Step 1 and Step 2
- ✓Multiple users and ease of use
- ✓Review process and annotation
- ✓Reporting

Stiki
Information Security

Principal Project Managers

Stiki – Information Security

Svana Helen Björnsdóttir

- Founder and CEO, Stiki ehf.
- Engineering PhD Candidate, Reykjavík University
- svana@stiki.eu
- www.riskmanagementstudio.com ; stiki.eu

Zurich University of Applied Sciences – ZHAW

Martin Rejzek

- Deputy Head, Safety – Critical Systems Research Lab
- martin.rejzek@zhaw.ch
- www.zhaw.ch/iamp/sks

Stiki
Information Security

Participants Logos

Stiki
Information Security

ORM Studio
Risk Management — Efficient and Effective

eurostars™

Zurich University
of Applied Sciences

zh
aw

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Education,
Research and Innovation SERI

Technology
Development Fund

Stiki
Information Security

Demonstration: STPA Analysis

Special thanks to Todd Pawlicki & co-authors for use of their STPA analysis.

Medical Physics
The International Journal of Medical Physics Research and Practice

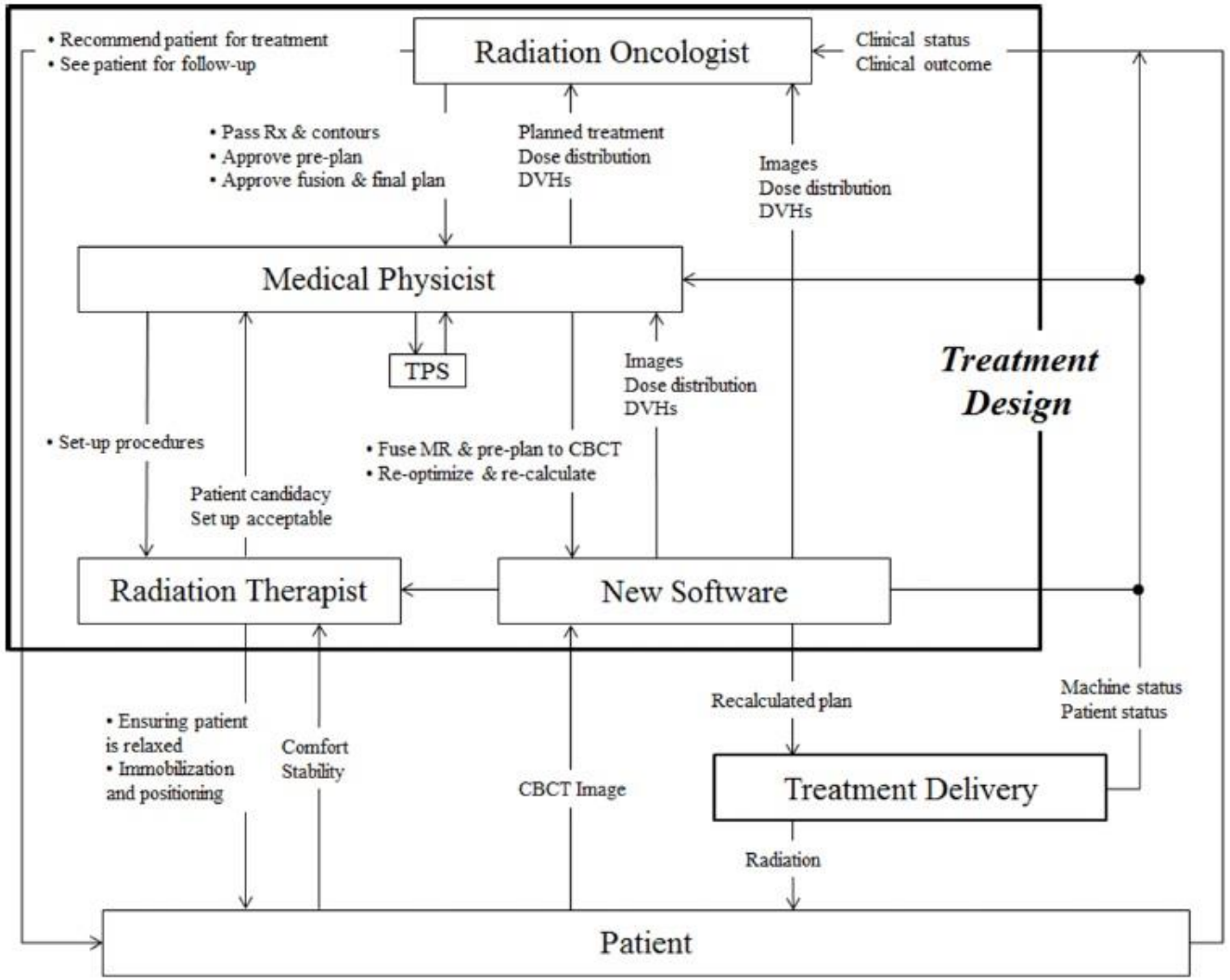
Application of systems and control theory-based hazard analysis to radiation oncology

Todd Pawlicki, Aubrey Samost, Derek W. Brown, Ryan P. Manger, Gwe-Ya Kim, and Nancy G. Leveson

Citation: Medical Physics **43**, 1514 (2016); doi: 10.1118/1.4942384
View online: http://dx.doi.org/10.1118/1.4942384
View Table of Contents: http://scitation.aip.org/content/aapm/journal/medphys/43/3?ver=pdfcov
Published by the American Association of Physicists in Medicine

Stiki
Information Security

Demonstration: STPA Analysis



Stiki
Information Security

Demonstration: STPA Analysis

TABLE I. List of the controllers, job functions, safety responsibilities, and associated control actions as part of the STPA for the new Linac-based radiosurgery procedure.

Controller	Function performed	Safety responsibilities	Control actions
Radiation oncologist	The radiation oncologist uses his medical and specialty knowledge when evaluating the patient for treatment and uses the dose distribution, DVHs, and imaging for setup and optimal treatment plan	• Ensure that radiation, the Rx and contours are appropriate to treat the patient's disease • Verify that the final plan and patient setup are acceptable prior to treatment • Observe and manage any unexpected complications during and after treatment	• Pass prescription and contours • Approve preplan • Approve fusion and final plan • Recommend patient for treatment • See patient for follow-up
Medical physicist	The medical physicist uses his knowledge of treatment planning system, fusion algorithms, and imaging techniques to prepare treatment plans and evaluate patient setup	• Ensure that the plan (Linac instructions) is able to be delivered without error and that equipment is functioning properly • Verify that the treatment plan meets the radiation oncologist's Rx and has all the necessary information for the radiation therapist	• Set-up procedures • Fuse MR and preplan to CBCT • Reoptimize and calculation • Send new plan to RT EMR • Schedule for treatment
Radiation therapist	The radiation therapist uses his clinical experience and knowledge to interact with and position the patient per the setup protocol and execute treatment per the treatment plan	• Ensure the patient is comfortable and follows instructions for treatment • Ensure that the patient is setup per the treatment plan and procedures are followed as designed • Verify that the equipment is functioning properly during the treatment	• Ensuring patient is relaxed • Immobilization and positioning • Acquire CBCT • Mode up final plan • Initiate treatment • Halt treatment

Stiki Information Security

Demonstration: STPA Analysis

TABLE II. STPA step 1 table of UCAs for the *medical physicist controller* (see Figs. 3 and 6 in the Appendix).

Control action	The control action is not given	The control action is given incorrectly	The control action is given at the wrong time or wrong order	The control action is stopped too soon or applied too long
Setup procedures	The SOPs are not communicated to the new radiation therapist when the radiation therapist changes linear accelerator coverage ($H1$, $H2$, $H5$)	The SOPs are incorrect or incorrectly communicated when the procedure is introduced into clinical use ($H1$, $H2$, $H5$) The SOPs do not get updated and/or communicated when there is a planned process modification ($H1$, $H2$, $H5$)	The CBCT-only SRS program is started before the SOPs are completed ($H1$, $H2$, $H5$)	The SOPs are finalized before getting input from all team members (radiation oncologists, medical physicists, radiation therapists, schedulers) ($H1$, $H2$, $H5$)
Fuse MR and preplan to CBCT	The medical physicist does not perform the fusion when the images (and MR preplan) are ready ($H1$)	The medical physicist fuses the images and MR preplan incorrectly when using the fusion software ($H1$)	The images are fused before the final or most recent CBCT is acquired and transferred for fusion ($H1$)	The fusion takes too long when transferring images or using the fusion software ($H1$)
Reoptimize and calculate	Suboptimal treatment occurs when a suboptimal MR pre-plan is scheduled for treatment ($H1$)	An inaccurate dose calculation is provided when the medical physicist uses the software to perform the calculation ($H1$)	N/A	Reoptimization or calculation takes too long when using the treatment planning software ($H1$) Reoptimization ends before completed after the medical physicist initiates the optimization ($H1$)

Stiki Information Security