1 Thema

KrisenPlan: **Plan**spiele für **Krisen**management in Rechenzentren

2 Zeitraum

Sommersemester 2015 und Wintersemester 2015/2016

3 Veranstalter

Dr. Johannes Neubauer <johannes.neubauer@tu-dortmund.de>, Tel. 7779
Dipl.-Inf. Stefan Naujokat <stefan.naujokat@tu-dortmund.de>, Tel. 7734
Dipl.-Inf. Michael Lybecait <michael.lybecait@tu-dortmund.de>, Tel. 7756
Prof. Dr. Bernhard Steffen <steffen@cs.tu-dortmund.de>, Tel. 5801
Informatik Lehrstuhl 5, Otto-Hahn-Straße 14, Raum 135/136
In Kooperation mit
Dr. Michael Neubauer <mine@kopv.de>, Fachexperte für Krisenmanagement in IT-Projekten

4 Aufgabe

Im Rahmen des Projekts ist ein rechnergestütztes Planspiel zu erstellen, das der Schulung des Personals eines Rechenzentrums für den methodischen Umgang mit Krisensituationen dient. Durch die weltweite Vernetzung und die permanente Nutzung von IT-Leistungen im Internet müssen die meisten Rechenzentren 365 Tage 24 Stunden verfügbar sein. Für viele Unternehmen aber auch für öffentliche Infrastrukturen werden daher erhebliche Anstrengungen unternommen, um das Ziel einer permanenten Verfügbarkeit zu erreichen.

Im Kern beziehen sich diese Sicherungsmaßnahmen auf folgende Bereiche:

- **Physische Sicherheit:**
  - Zugangskontrollen
  - Vorfeldsicherung (z.B. Umzäunung, Kameraüberwachung)
  - Sicherungen gegen Gewalteinwirkung
- **IT-technische Redundanz:**
  - Raid-Speichersystem
  - Cluster-Computersysteme
  - Mehrfachauslegung von Standorten
- **Infrastruktursicherung:**
  - Notstromaggregate
  - Unterbrechungsfreie Stromversorgung
- **Organisatorische Maßnahmen:**
  - Bereitschaftsdienst (z.B. über sog. Krisentelefone)
  - Eskalationslisten mit Verantwortlichen
  - Protokolle für Fehlerbehebung in Standardsituationen (z.B. defekte Festplatte)
  - Dokumentation

Abbildung 1: Krisensituation bei der KDVZ Citkomm.

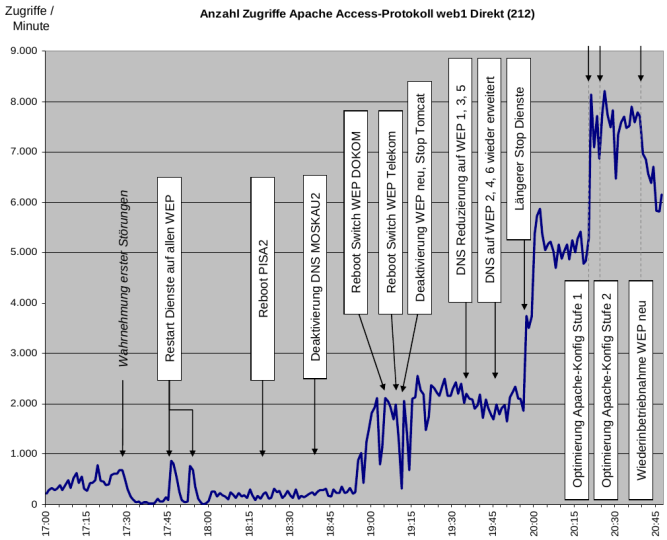

Abbildung 2: Analyse einer Krisensituation (siehe [4]).

Alle diese Punkte basieren auf dem Konzepte einer strukturierten Risikoanalyse und einem daraus abgeleiteten Maßnahmenplan, der die induzierten Risiken systematisch reduziert. Offensichtlich wird damit ein Ausfall unwahrscheinlich, ohne dadurch unmöglich zu werden (siehe Abb. 1). Katastrophen wie der Reaktorunfall in Fukushima zeigen deutlich, dass systematische Redundanz- und Sicherheitskonzepte keine Garantie gegen Ausfälle und Störungen bieten können. In diesem Fall ist ein generisches Notfallkonzept notwendig, das sich nicht auf eine spezifische vorhergesehene Fehlersituation (einem sog. Fehlermodell) stützt, sondern flexible organisatorische und methodische Werkzeuge bereitstellt, die von einer gut trainierten Betriebsmannschaft in nicht berücksichtigten Fehlersituation systematisch angewendet werden können.

Während es z.B. für Flugzeuge, Schiffe oder Atomreaktoren hochentwickelte Simulations- und Trainingskonzepte gibt, kommen derartige Techniken im Bereich von IT-Systemen im Allgemeinen und von Rechenzentren im Besonderen bisher nicht zum Einsatz. Anders als bei Schiffen oder Flugzeugen werden Rechenzentren nicht als standardisierte Systeme implementiert. Die Modellierung eines Rechenzentrums mit all seinen Bedienelementen ist zwar grundsätzlich denkbar aber unwirtschaftlich ebenso wie eine physikalische Nachbildung. Die Nutzung der Redundanzsysteme für einen Test ist nicht praktikabel, da sie in laufende Betriebsabläufe eingreifen und Sicherheitskonzepte untergraben würde. Unser Kooperationspartner verfügt über mehr als 25 Jahren Erfahrung im Bereich des Rechnerbetriebs und beschäftigt sich seit vielen Jahren systematisch mit deren Bewältigung (siehe Abb. 2). Dieses Wissen soll insbesondere dazu dienen die Studenten bei der Entwicklung eines Spielmodells zu begleiten.

Bei der Bewältigung von unvorhergesehenen Fehlersituationen ist, zumindest im Fall von Rechenzentren, eine Modellierung der Betriebsumgebung nicht primär erforderlich, da die Erfahrung zeigt, dass es bei der Bewältigung von Krisen weniger an der Routine in der Bedienung der Steuersysteme mangelt. Es zeigt sich viel mehr, dass es Probleme in der Interaktion der vielen Administratoren, der systematischen Analyse und der Dokumentation von Maßnahmen gibt. Darüber hinaus ist die Interaktion mit dem Management und der Öffentlichkeit problematisch.

Vor dem Hintergrund dieser Überlegung ist die Entwicklung eines computergestützten Planspiels eine flexible und wirtschaftliche Alternative. Die primäre Zielsetzung liegt nicht in dem Training von Routineabläufen, sondern von typischen Krisensituationen. Die technischen Dimension soll durchaus beherrschbar sein. Es geht darum unerwartete Ereignisse unter nicht kontrollierbaren externen Randbedingungen (Gefährdungen, wirtschaftliche Schäden, öffentliches Interesse, etc.) zu modellieren die Stress auf die Gruppe ausüben. Hierbei werden Randbedingungen und Einflüsse in die Kategorien *modellintern* (z.B. Hardwaredefekte, Preiseinbrüche) und *modellfremd* (z.B. Forderungen des Managements oder der

Öffentlichkeit) eingeteilt.

Ziel

Die Spielsituation soll ein Team von Administratoren umfassen, das unter zeitlichem Druck steht und in seiner Analyse der auftretenden modellinternen technischen sowie wirtschaftlichen Probleme durch modellfremde Spielteilnehmer wie Kunden, Management und interessierte Öffentlichkeit beeinflusst (bzw. gestört) wird.

Im Rahmen des Projekts ist eine Startzustand eines funktionierenden Rechenzentrums so zu modellieren, dass eine für die Spieler realistische, aber leicht zu überblickende Spielsituation entsteht. Dabei sind die gängigen Rechenzentrumsbestandteile abstrakt zu beschreiben und in ihrer Spielrelevanz zu klassifizieren. Mögliche Modellbestandteile können sich z.B. auf Hardware (Notstrom, Klima, Server, Speicher etc.), Messgrößen (Stromverbrauch, Temperatur, Benutzerzahlen, Prozesse, Anfragen etc.) und Software (Dienste, Versionen, Abbrüche, Ausgaben etc.) beziehen. Diese Modellbestandteile bilden die Spielobjekte die durch Abhängigkeiten und Funktionen in einen dynamischen Zusammenhang gestellt werden. Die Spieler interagieren mit dem System in dem sie diese Abhängigkeiten und Funktionen im Rahmen eines Regelwerks verändern.

Das im Rahmen der Projektgruppe zu erstellende Planspiel soll aus einer Einarbeitungsphase, in der die Spieler (das RZ-Team) das System im Normalzustand auf ein einstellbares Ziel hin optimieren. Das eigentliche Training besteht aus einer Krisenphase in der das Team ein System steuern muss, das aus fehlerhaften Modellbestandteilen besteht. Das Team muss dabei gemeinsam die modellinternen Fehler (z.B. Hardwaredefekt) analysieren und sich gegenüber den modellexternen Störungen (z.B. Management) behaupten. Das Team bekommt vor dem Training methodische Grundlagen vermittelt, wie mit solchen Situationen umzugehen ist. Bei konsequenter Anwendung dieser Methodik soll eine schnelle Auflösung der Fehlersituation möglich sein.

Technologien

Prozessmodellierung

Modellgetriebene Softwareentwicklung (Model-Driven Development, MDD) bietet neben der aus Informatiker-Sicht vorteilhaften Möglichkeit, modellbasierte Verifikationstechnologien anwenden zu können (wie z.B. Model-Checking) auch den Vorteil, für Nicht-Programmierexperten domänenspezifische Konzepte in Form von Workflows einfach umzusetzen. Am Lehrstuhl für Programmiersysteme existiert mit dem jABC4 [5] ein Framework, das dieses Vorgehen inklusive Validierungsmechanismen [3] untertützt sowie durch Codegeneratoren in verschiedenen Umgebungen Ausführbarkeit ermöglicht.

Domänenmodellierung

Die Domänenmodellierung ist ein wichtiger Bestandteil der Anforderungsanalyse in einem Softwareprojekt. Die *Dynamic Web Application* (DyWA) [6] bietet zusätzlich einen agilen Umgang mit den Datenstrukturen einer Webanwendung und integriert das Domänenmodell reibungslos als Prozessbausteine in die Geschäftsprozesse von jABC4 ein.

Krisenmanagement

Für die Modellierung der Spielsituation sind neben wenigen für einen Informatiker leicht zu modellierenden Aspekten der Hardware und der Bedienung eines Rechenzentrums vor allem methodische Kenntnisse bzgl. der Bewältigung von Krisensituationen erforderlich [7]. Diese werden in der Seminarphase erarbeitet und auf das vorliegende Problem angewendet.

Die Bewältigung alltäglicher wie auch schwieriger Probleme ist in [2] überblicksartig dargestellt. Dabei wird deutlich, dass es bei der Bewältigung von Krisen keine Patentrezepte gibt. Gleichzeitig wird offenbar, dass die spielerische Auseinandersetzung mit typischen Problemsituationen zwei Vorteile mit sich bringt: (1) Die Wiederholbarkeit von Planspielen und das regelmäßige Training führen zu einer Reduzierung von Stresssituationen und unterstützen so eine rationale Bewältigung von Krisen. (2) Aus der Beobachtung der Spielabläufe lassen sich wertvolle Erkenntnisse für organisatorische und methodische Werkzeuge ableiten.

Damit diese Vorteile erzielt werden können, muss das Modell und das Planspiel bestimmten methodischen Grundregeln entsprechen, die u.a. in der Arbeit von [1] analysiert und dargestellt werden.

5 Teilnahmevoraussetzungen

Vorausgesetzt werden fundierte Kenntnisse in mindestens einer objektorientierten Programmiersprache, bevorzugt Java sowie elementare Kenntnisse über Modellierungstechniken, wie sie z.B. in den Vorlesungen „Formale Methoden des Systementwurfs“, „Virtualisierung und Compilation “, „Softwarekonstruktion“ und „Dienstleistungsinformatik“ vermittelt werden. Wünschenswert sind zudem Kenntnisse im Umgang mit integrierten Entwicklungsumgebungen (IDEs), Versionskontroll- und Build Management Systemen sowie Kenntnisse über Geschäftsprozesse und Informationssysteme.

6 Minimalziel

Im Rahmen der PG soll ein computergestütztes Planspiel als Webanwendung erstellt und exemplarisch eingesetzt werden, das die o.g. Phasen *Einarbeitung* und *Krisensituation* geeignet abbildet.

7 Literaturverzeichnis

[1] K. Autenrieth. Spiele und ihre Regeln. Master thesis, Universität Leibzig, 2013.

[2] D. Dörner. *Die Logik des Misslingens: strategisches Denken in komplexen Situationen.* Rororo. Rowohlt, 2003.

[3] B. Jonsson, T. Margaria, G. Naeser, J. Nyström, and B. Steffen. Incremental Requirement Specification for Evolving Systems. *Nordic J. of Computing*, 8(1):65–87, Mar. 2001.

[4] M. Krengel and F. Albrecht. Störungen bei der Bereitstellung der Wahlergebnispräsentation (WEP) der KDVZ Citkomm zur Kommunalwahl 2009. 2009.

[5] J. Neubauer. *Higher-Order Process Engineering.* Phd thesis, TU Dortmund, July 2014.

[6] J. Neubauer, M. Frohme, B. Steffen, and T. Margaria. Prototype-driven development of Web Applications with DyWA. In *Leveraging Applications of Formal Methods, Verification and Validation. Technologies for Mastering Change*, pages 56–72. Springer Berlin Heidelberg, 2014.

[7] M. Neubauer. *Krisenmanagement in Projekten.* Springer, 3 edition, 2010.

8 Rechtlicher Hinweis

Die Ergebnisse der Projektarbeit und die dabei erstellte Software sollen der Fakultät für Informatik uneingeschränkt für Lehr- und Forschungszwecke zur freien Verfügung stehen. Darüber hinaus sind keine Einschränkungen der Verwertungsrechte an den Ergebnissen der Projektgruppe und keine Vertraulichkeitsvereinbarungen vorgesehen.