Trials@uspto.gov
571-272-7822

Paper No. 12
Entered: September 11, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SERVICENOW, INC.,
Petitioner,

v.

BMC SOFTWARE, INC.,
Patent Owner.

Case CBM2015-00107
Patent 7,062,683 B2

Before JUSTIN T. ARBES, JENNIFER MEYER CHAGNON, and TIMOTHY J. GOODSON, *Administrative Patent Judges.*

GOODSON, *Administrative Patent Judge.*

DECISION
Denying Institution of Covered Business Method Patent Review
37 C.F.R. § 42.208

I. INTRODUCTION

Petitioner ServiceNow, Inc. filed a Corrected Petition (Paper 4, "Pet.") requesting covered business method patent review of claims 1–3, 12, 14, 21, 22, 24–26, 35, 37, 44, 45, 56–58, 67, 69, 76, 77, 79, 80, 83, 85, and 88–90 of U.S. Patent No. 7,062,683 B2 (Ex. 1001, "the '683 patent"). Patent Owner BMC Software, Inc. filed a Preliminary Response (Paper 11, "Prelim. Resp.").

We have jurisdiction under 35 U.S.C. § 324. Pursuant to 35 U.S.C. § 324(a), the Director may not authorize a covered business method patent review unless the information in the petition, if unrebutted, "would demonstrate that it is more likely than not that at least 1 of the claims challenged in the petition is unpatentable." As explained below, we do not institute a covered business method patent review because the information presented in the Petition does not establish that the '683 patent qualifies as a covered business method patent.

A. The '683 Patent

The '683 patent relates to a method of using fault models to analyze error conditions in an enterprise computing system. Ex. 1001, 1:5–10.

The '683 patent explains that the reliability of complex enterprises depends in large part on detecting and managing operational problems, such as hardware or software failures. *Id.* at 1:21–27. As an enterprise incorporates more monitored components, the occurrence of observable events greatly increases. *Id.* at 1:30–35. Many of these are "sympathetic events" that are generated as a result of the underlying problem. *Id.* at 1:35–38. The '683 patent explains:

> For example, a router failure may generate a "router down" event and a large number of "lost connectivity" events for

> components that communicate through the failed router. In this scenario, the router failure is the fundamental or "root cause" of the problem and the lost connectivity events are "sympathetic" events.

Id. at 1:42–47. These sympathetic events complicate the task of identifying the cause of a problem. *Id.* at 1:35–38. According to the '683 patent, "up to 80% of a network's down-time is spent analyzing event data to identify the underlying problem(s)." *Id.* at 1:48–50.

The approach described in the '683 patent uses a combination of up-stream analysis and down-stream analysis on an impact graph to identify root cause faults separately from other notifications, many of which may be sympathetic. *Id.* at 4:33–40. Figure 1 is reproduced below:

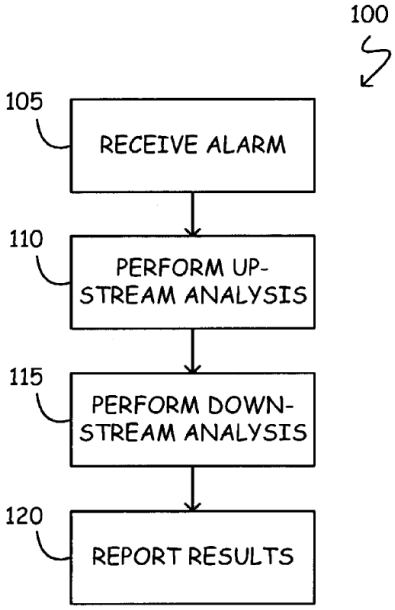

FIG. 1

Figure 1 is a flowchart showing the steps of model based reasoning (MBR) approach 100. *Id.* at 3:12–14, 4:31–33. As depicted by block 105 in Figure 1, the process begins when an alarm is received that provides notification of an event. *Id.* at 4:40–41.

In block 110, an up-stream analysis of the impact graph is performed beginning with the node that received the event notification, the effect of which may be to modify the "status value" of up-stream nodes. *Id.* at 4:43–46. Up-stream analysis

> proceeds, in an iterative fashion, up the graph until (1) there are no more up-stream nodes; or (2) a node's status value does not change as a result of the node's inference policy; or (3) the inferred status value for a node is different from the node's measured status value.

Id. at 6:3–7.

Next, in block 115, down-stream analysis is performed beginning with the furthest up-stream node whose status value was modified in the up-stream analysis. *Id.* at 4:46–50. The effect of the down-stream analysis may be to modify the "impact value" of nodes down-stream of the starting node. *Id.* at 4:50–53. In the down-stream analysis, the "starting node's impact policy, and each successive immediately down-stream node's impact policy[,] are then evaluated until (1) there are no more down-stream nodes or (2) a down-stream node's impact value does not change as a result of the evaluation." *Id.* at 6:56–60.

In block 120, identification of root-cause failures and sympathetic event notifications can be reported. *Id.* at 4:60–63. Generally, the root-causes are the furthest up-stream nodes having a status value indicative of failure. *Id.* at 4:63–67. Nodes down-stream from the root cause and whose impact values indicate that they were impacted by the root-cause failure can also be shown, but it may be beneficial for these event notifications of impacted nodes to be masked or displayed in a different manner than the root causes. *Id.* at 5:3–8.

The ’683 patent illustrates the method of Figure 1 by applying it to an exemplary enterprise. *See id.* at 9:7–11. In particular, Figure 7, which is reproduced below, depicts an impact graph for an enterprise consisting of automatic teller machines (ATMs) coupled to a central banking facility through a satellite communications system. *Id.* at 7:31–34, 8:43–45.

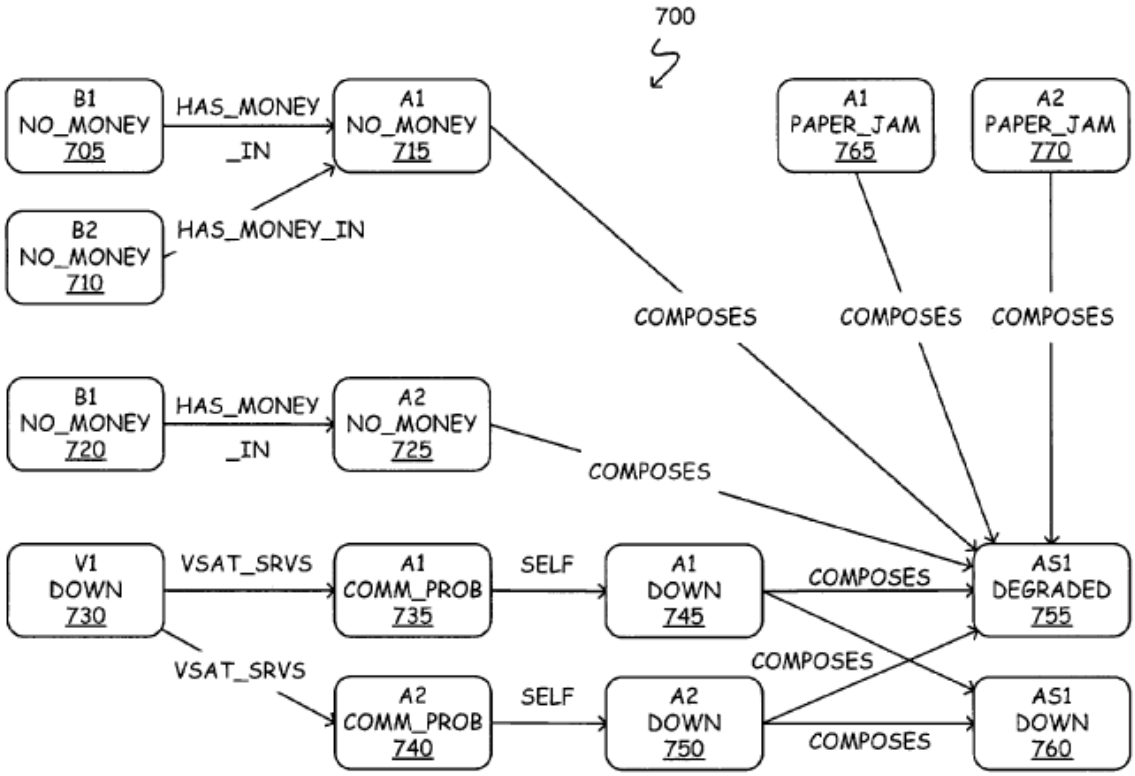

FIG. 7

The illustrative example begins when, in accordance with block 105 of Figure 1, an alarm event associated with node 715 is received. *Id.* at 9:10–11. The event notification causes the status value of node 715 to be measured “true,” which indicates a failed status. *Id.* at 9:50–54.

In the up-stream processing of block 110, the inference policies of nodes 705, 710 are evaluated. *Id.* at 9:12–45. In this example, the status values of nodes 705, 710 are inferred to be “true” because the immediately

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.