Ulmer Informatik-Berichte Nr. 2003-02

Supporting Workflow Schema Evolution By Efficient Compliance Checks*

Stefanie Rinderle, Manfred Reichert, Peter Dadam
University of Ulm, Computer Science Faculty,
Dept. Databases and Information Systems,
89069 Ulm, Germany
E-Mail: {rinderle, reichert, dadam}@informatik.uni-ulm.de

Abstract

Process-oriented support of collaborative work is an important challenge today. At first glance, *Workflow Management Systems (WfMS)* seem to be very suitable tools for realizing team-work processes. However, such processes have to be frequently adapted, e.g., due to process optimizations or when process goals change. Unfortunately, runtime adaptability still seems to be an unsolvable problem for almost all existing WfMS. Usually, process changes can be accomplished by modifying a corresponding (graphical) workflow (WF) schema. Especially for long-running processes, however, it is extremely important that such changes can be propagated to already running WF instances as well, but without causing inconsistencies and errors. In addition, team work often requires ad-hoc process modifications, i.e., individual changes of single WF instances. The paper presents a general and comprehensive correctness criterion for ensuring compliance of in-progress WF instances with a modified WF schema. For different kinds of WF schema changes, it is precisely stated, which rules and which information are needed at mininum for satisfying this criterion.

1 Introduction

Computer Supported team work has become more and more important during the last years since humans and machines can share their power and spirit. The various software systems to support collaborative work can be summarized as *Computer Supported Cooperative Work (CSCW)* systems. CSCW systems can be classified, for example, according to the degree of distribution of *time* and *place* the team members work at (cf. Table 1).

One of the most powerful technologies within this classification framework is offered by *Workflow Management Systems (WfMS)*. WfMS support team members working on a complex

*This work was done within the research project "Change management within adaptive workflow management systems", which has been founded by the German Research Community (DFG)

Table 1: Classification Of CSCW (cf. [24])

		time of interaction	
		same time	*different time*
presence of team members	*same place*	meeting support	team room / shift work
	different places	desktop conferences multicast seminar	E-Mail, collaborative editor Workflow-Management

task at distributed places and at different points in time. Furthermore, they offer a promising technology for process-oriented coordination of (distributed) team work [14], i.e., they allow to organize team work in a process-oriented manner and across organizational boundaries. For each workflow (WF) type to be supported (e.g., concerning the treatment of patients in a hospital or the design of a sales promotion), a corresponding *WF schema* S has to be defined. It comprises a set of activities with associated application components and with explicitly defined control and data flow between them. At run-time, new *WF instances* $I_1, \ldots, I_n$ can be created from this WF schema and be executed according to the defined process logic.

1.1 Problem Description

Intuitively, *team-work processes* are of complex structure and long duration, e.g., engineering processes or therapeutical treatments. Therefore *changes* may take place very often. Consequently, the team-work processes have to be rapidly adapted [1]. However, today's WfMS lack almost totally of supporting adaptive processes. Either they only allow changes at the WF schema level without taking running WF instances into account[1] (e.g., MQ Series Workflow and Vitria BusinessWare) or they *propagate* such WF schema changes to running WF instances without any consistency checks (e.g., Staffware). However, doing so very often leads to heavy-weight consequences like deadlocks or program crashes due to the invocation of activity components with missing input data. Although this fundamental problem has been recognized in the WF literature (e.g., [5, 11, 13, 21]), the suggested solutions are either too restrictive or not applicable in practice (cf. Section 6). Thus, when applying today's WF technology we lose just the flexibility which is indispensable for team-work needs. To overcome the limitations of existing WfMS and research approaches, basically, we need a formal framework to support WF schema modifications and their propagation to running WF instances. Note that presently, almost all commercial WfMS and most of the research prototypes [5, 25] lack just this clear theoretical basis.

Intuitively, a WF schema change can be propagated to a WF instance if this is not "contradictory" to its previous execution and would not cause errors or inconsistencies. Then this instance is said to be *compliant* with the modified schema. A naive solution would be to try to replay *all* events that have taken place during the execution of this WF instance so far on the

[1] i.e., only allowing future WF instances to be run according to the new version of the WF schema

changed WF schema as well. If this is possible, compliance can be guaranteed. Otherwise, the change is in conflict with previous instance execution. Apart from the fact that replaying all execution events may cause a performace penalty at the presence of a large number of WF instances this approach works well as long as no loops have to be considered. However, it is far too restrictive in conjunction with cyclic process structures (which are very typical for team-work processes). More precisely, changes that may be applied in the current state of a WF instance may be "contradictory" to previous loop iterations since the respective execution history has already logged them without taking the change into account. Therefore replaying this history on the changed WF schema is doomed to failure. To prohibit those potentially long-running instances from migrating to the new WF schema is out of touch with reality. Furthermore, using the whole information about previous execution events is very expensive. Note that there are real-world applications with hundreds up to thousands of WF instances of a given WF type. Each of them comprises extensive execution histories (see e.g., [16]) of which much data is totally unnecessary for checking compliance.

1.2 Contribution

The paper presents a comprehensive and theoretically sound approach for compliance checking in connection with WF schema changes. Comprehensive means that we do not needlessly exclude WF instances from their migration to a changed schema (as described above). In this context, a formal underpinning is indispensable to enable the WfMS to automatically decide whether a given WF instance is compliant with the new WF schema or not; i.e., whether it can be smoothly migrated to it. In addition, it must be clear which information is needed at minimum for compliance checking. In most approaches from research, however, this is not precisely stated, hence leading to either (over) restrictive solutions or to "implementation holes" later on (for a detailed discussion see Section 6). Other approaches, in turn, assume that all history data of a WF instance must be taken for checking compliance [5, 13, 21] which is, in general, too expensive as described. In this paper, we proceed in two major steps and make the following contributions:

- We first define a comprehensive compliance property which is independent from the used WF meta model and its underlying operational semantics. Furthermore, it abolishes the restrictions of existing approaches (especially in conjunction with loops and data flow).
- We precisely state under which conditions compliance of a WF instance with a changed WF schema can be guaranteed. These conditions depend on the current state of WF instances as well as on the kind of change operation applied. In any case, the needed information is shrunken to a minimum size that way.

The present work is embedded in the ADEPT project, which aims at the flexible support of enterprise-wide work processes [17]. We have developed and implemented advanced concepts for the modeling, execution, and monitoring of workflows as well as for the ad-hoc changes of in-progress WF instances [10]. The WfMS prototype implemented by our team has been

used by several groups to realize flexible process-oriented applications [3, 15]. In previous publications concerning ADEPT, we focused on ad-hoc changes of individual WF instances [17]. Our main emphasis was on the provision of high-level change operations (and the related WF schema transformations) and on correctness, scalability, and implementation issues arising in this context.

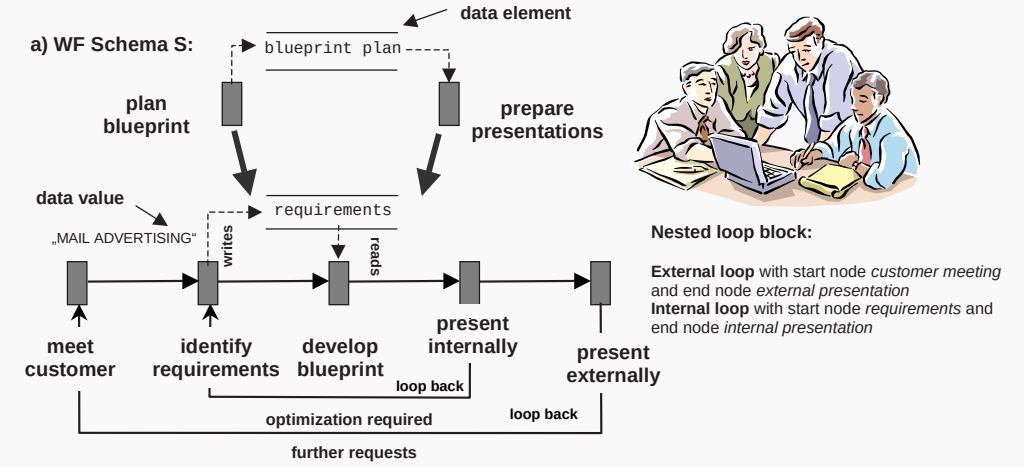
In the current paper, we develop the formal underpinning of our current work on WF schema evolution, focussing on issues related to efficient compliance checks. In Section 2 we present a generic and comprehensive compliance property which abolishes the restrictions of present approaches. Sections 3 and 4 provide simple compliance checks for control as well as data flow changes. We summarize further relevant issues in Section 5 and discuss related work in Section 6. Finally, we sketch the main contributions presented in this paper in Section 7.

2 A Comprehensive Compliance Property

To enable the WfMS to decide whether a particular WF instance can be correctly migrated to a changed WF schema or not, we need appropriate rules. In addition, it is important that these rules can be efficiently checked. Obviously, information about the execution performed so far is needed for this purpose. Many WfMS log this information within an *execution history*, which is kept for each WF instance. This history is also required, for example, when tracking the execution of a WF instance or when (partially) rolling back WF instances in case of failures [14].

A straightforward, but restrictive approach, which has been used by several groups (e.g., [5, 21]), would be to check whether the complete execution history of a WF instance could have been also produced when executing the WF instance based on the changed WF schema (*restrictive compliance property*). This might cause a performance penalty due to the possibly large volume of history data (see e.g., [16]) which has to be scanned. Apart from performance, following this approach, WF instances might be excluded from migrating to the changed schema, though this would not lead to inconsistencies or errors in the sequel. Generally, the restrictive compliance property leads to problems when WF schema changes affect loop structures. As an example take Fig. 1 with WF schema S, initially consisting of a nested loop block with one external and one internal loop (including 3 activities and one data dependency). Assume that new activities `plan blueprint` and `prepare presentations` (with one data dependency between them) shall be added to WF schema S.

This change can be easily accomplished in a correct and consistent manner at the WF schema level. But how to treat in-progress WF instances (with schema S) when applying the change? Assume that `Instance 1` is described by the execution history shown in Fig. 1b. Following the restrictive approach, the intended change could not be propagated to `Instance 1` of schema S since no history entries for `plan blueprint` and `prepare presentations` have been written within the first (completed) iteration of the external and the internal loop. Hence, `Instance 1` is not compliant with the new schema when taking the restrictive compliance criterion. Only WF



b) Execution History of Instance 1:

<START(meet customer, 1st it), END(meet customer), START(identify requirements, 1st it), END(identify requirements, write(requirements, "MAIL ADVERTISING"), START(develop blueprint, read(requirements, "MAIL ADVERTISING"), END(develop requirements), START(present internally), END(present internally, optimization required = FALSE), START(present externally), END(present externally, further requests = TRUE), START(meet customer, 2nd it), END(meet customer), START(identify requirements, 2nd it), END(identify requirements, write(requirements, "TV advertising")>

c) Execution History of Instance 2:

<START(meet customer, 1st it), END(meet customer), START(identify requirements, 1st it), END(identify requirements, write(requirements, "RADIO ADVERTISING"), START(develop blueprint, read(requirements, "RADIO ADVERTISING"))>

d) Reduced Execution History of Instance 1:

<START(meet customer, 2nd it), END(meet customer), START(identify requirements, 2nd it), END(identify requirements, write(requirements, "TV advertising")>

Figure 1: Team-Oriented Creation Of A Marketing Concept (Example)

instances, which are in the first iteration of both – the internal and the external loop – could be adequately treated in this case. From a practical viewpoint, however, in most cases it will be too restrictive to prohibit change propagation for in-progress or future loop iterations only because their previous execution is not compliant with the new schema. Think of, for example, medical treatment cycles running for months or years. Any WfMS which does not allow propagating schema changes (e.g., due to the development of a new drug) to running instances (e.g., related to patients expecting an optimal treatment!) would not be accepted be a medical team at all.

What adds insult to injury is that the restrictive compliance property is not always suitable when considering data flow changes as well. As an example consider `Instance 2` with the execution history shown in Fig. 1c. Activity `develop blueprint` has been already started and therefore has read data element `requirements`. Assume that the read data link of activity `develop blueprint` is re-mapped from `requirements` to another data element. For this instance, the activity component associated with activity `develop blueprint` is run with input data `requirements` though the respective data link is not present any longer in the new schema.

In summary, the support of loops is indispensable for any WfMS. To enable the WfMS to invoke arbitrary application components, it is also important to adequately handle data flow and data flow changes. The challenge is to define a compliance property, which embraces these aspects in a uniform manner as well. The key to solution with respect to loops is to be able to differentiate between completed and future executions of loop iterations. From a formal point of view there are two possibilities. One approach is to logically treat loop structures as being equivalent to respective linear sequences. Doing so allows to apply the restrictive compliance property (with full history information). The other approach is to maintain the loop construct but to restrict the evaluation to the relevant parts of the execution history. We have adopted the second approach since it facilitates the handling of nested loops and loops with an unknown number of iterations.

Definition 1 (Reduced Execution History $\mathcal{H}_{red}$) *Let I be a WF instance with complete execution history $\mathcal{H} =< e_0, \ldots, e_k >$, where $e_0, \ldots, e_k$ denote start and end events of all activity executions related to I. (In conjunction with loop executions there may be several entries for one activity.) – The reduced execution history $\mathcal{H}_{red}$ is obtained as follows: In the absence of loops $\mathcal{H}_{red}$ is identical to $\mathcal{H}$. Otherwise, it is derived from $\mathcal{H}$ by discarding all history entries related to other loop iterations than the last one (completed loop) or the actual iteration (running loop).*

Fig. 1d depicts the reduced execution history derived from the execution history shown in Fig. 1b. From this example we can also see how Def. 1 works in conjunction with nested loops. Taking Def. 1 we now present a comprehensive compliance property for WF schema evolution. According to this property, a WF instance is compliant with a changed schema iff the reduced execution history can be produced on the modified schema as well.

Axiom 1 (Comprehensive Compliance Property) *Let I be a WF instance on WF schema S with execution history $\mathcal{H}$ and reduced execution history $\mathcal{H}_{red}$. Assume further that a change Δ transforms the WF schema S into the correct WF schema S'. Then I is said to be compliant with S' iff*

- *$\mathcal{H}_{red}$ can be produced on S' as well*
- *each started or finished activity (of the respective WF instance) would have read and each finished activity would have written the same data element values also on the new schema.*

Axiom 1 is valid for all WF execution models which store information about the previous execution of instances. Examples include Activity Nets as used by MQ Series Workflow and the WF models applied in BREEZE [21], WASA$_2$ [25], and ADEPT [17]. Approaches only maintaining state information about currently activated or running activities (e.g., Petri Nets) are discussed in Section 6.

We have now introduced a universally valid correctness criterion for ensuring compliance of WF instances with a changed WF schema, which is fundamental for any adaptive WfMS. The challenging question is how to quickly decide Axiom 1 without need for taking the (whole) extensive history information into account[2]. One approach which is worth to follow is to design the WF execution model (including its formal and operational semantics) in such a way that efficient compliance checks avoiding access to the complete execution history become possible. For this, at the WF instance level we use a sophisticated marking approach where activity markings represent a consolidated and compact view on the execution history of a particular WF instance. In addition, when checking compliance we exploit the semantics of the applied change operations. Due to lack of space, in this paper we discuss relevant issues along the ADEPT WF model. The presented concepts, however, are not restricted to it. Basic design principles and the achieved compliance criteria can be transferred to other WF meta models (e.g., [21, 25]) as well.

3 Checking Compliance With Control Flow Changes

In this section we provide easy to check state conditions for WF instances which allow the WfMS to ensure compliance according to Axiom 1. At first, we give an (informal) overview about the WF meta model [17] assumed in this paper. From the very beginning, this meta model was designed with the perspective to change in-progress WF instances at runtime.

3.1 Control Flow Basics in ADEPT

ADEPT allows to model all relevant WF aspects, like control and data flow, work assignments, or time constraints [4, 17].

Control Flow Modeling. The flow of control is internally represented by attributed WF graphs with distinguishable node and edge types. As shown in earlier publications [17], this eases efficient correctness analysis (e.g., for the absence of ,,undesired" cycles causing deadlocks) as well as the interpretative execution of WF models. For this, we use a block concept, for which control blocks (sequences, branchings, loops) can be nested but must not overlap (see Fig. 2). To increase expressiveness, in addition, synchronization edges (SyncE) can be used to define "wait-for" relations between parallel nodes. In Fig. 2, for example, the target node `L` of the sync edge `D` $\rightarrow$ `L` may be only activated if `K` has been finished and if `D` has been either completed or the branch containing `D` is not selected for execution (i.e., `D` has been skipped). Formally, a control flow schema `S` is defined as follows:

[2]This problem is comparable to serializability of transactions, which is ensured by suitable synchronization methods, i.e., the defined compliance criterion (Axiom 1) can be considered as a general correctness criterion (like serializability) for which we have to find suitable checking routines.

Definition 2 (Control Flow Schema) *A tuple S = (N, D, NT, CtrlE, SyncE, LoopE, DP, EC) is called a (correct) control flow Schema if the following holds:*

- *N is a set of activities and D a set of process data elements*
- *NT:* $N \mapsto$ {`StartFlow, EndFlow, Activity, AndSplit, AndJoin, XOrSplit, XOrJoin, StartLoop, EndLoop`}
- *CtrlE* $\subset N \times N$ *is a precedence relation representing "normal" control dependencies between sequential activities*
- *SyncE* $\subset N \times N$ *is a precedence relation between activities of parallel branches*
- *LoopE* $\subset N \times N$ *is a set of loop backward edges*
- *DP:* $N \mapsto D \cup$ {`UNDEFINED`} *(global process data element indicating the branch to be selected when finishing an XOR-Split, DP(n) =* `UNDEFINED` *if NT(n)* $\neq$ *XOR-Split)*
- *EC: CtrlE* $\mapsto$ *EdgeCode* $\cup$ {`UNDEFINED`} *(selection code of control edges at an XOR-Split)*

Informally, a WF Schema S is correct iff
• S_{fwd} = (N, CtrlE, SyncE) is an acyclic graph, i.e., the use of control and sync edges must not cause undesired cycles leading to deadlocks (for details see [17]),
• for each split (loop start) node there is a unique join (loop end) node, and
• S is structured following a block concept, for which control blocks (sequences, branchings, loops) can be nested but must not overlap.

The ADEPT approach for control flow modeling is somewhat comparable to BPEL4WS (Business Process Execution Language for Web Services) [6], but with a more restricted use of links (called sync edges in our approach). The use of sync edges is combined with a precise formal and operational semantics and therefore enables appropriate consistency checking at buildtime as well as at runtime.

Workflow Execution. Based on a given WF schema `S`, new WF instances can be created and started. Similar to firing rules in Petri Nets, the marking of a WF instance is determined by well defined marking and execution rules (cf. Fig. 2d). As opposed to Petri Nets, logically, for each WF instance its own marking is maintained based on the related WF schema. Markings can be considered as a very compact and space-efficient representation of $\mathcal{H}_{red}$ (cf. Def. 1). In addition, except loop backs, the markings of already passed regions are maintained (cf. Fig. 2b), which is very useful for compliance checking as we show in the following. Furthermore, activity nodes of non-selected execution branches are marked as `SKIPPED`.

For each activity, its status is initially set to `NOT_ACTIVATED`. It is changed to `ACTIVATED` when all preconditions for its execution are met (cf. Fig. 2d). If so, the activity is released as a work task and inserted into user worklists. When selecting this activity for execution its status changes to `RUNNING`. The corresponding work items are then removed from other user

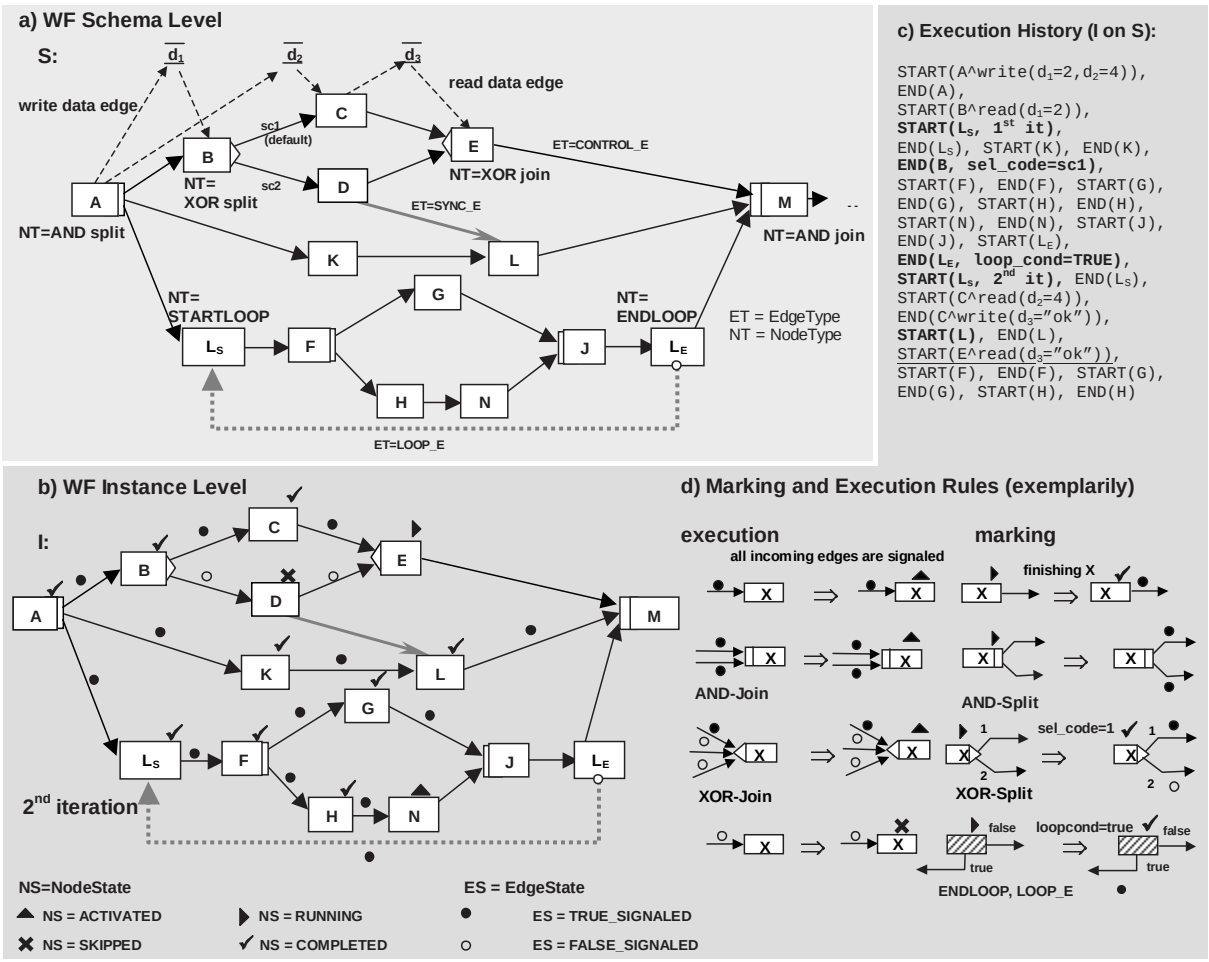


Figure 2: Modeling and Execution of Workflows in ADEPT

worklists and an application component associated with this activity is started. At successful termination, activity status passes to `COMPLETED`. Otherwise, if the scheduler recognizes that this activity cannot be selected for execution any longer, its status will change to `SKIPPED` (e.g., activity `D` of instance `I` in Fig. 2b). Edges are initially marked with `NOT_SIGNALED`. During WF execution their status either changes to `TRUE_SIGNALED` or `FALSE_SIGNALED`. Finally, if a loop condition evaluates to true, the marking of the corresponding edge (with type `LOOP_E`) is changed to `TRUE_SIGNALED` (cf. Fig. 2d) and the markings of all activities/edges of the loop body are reset to `NOT_ACTIVATED`/`NOT_SIGNALED`. Otherwise the loop is left whereas the actual markings of the loop body remain. Formally, a WF instance `I` is defined as follows:

Definition 3 (WF Instance) *A WF instance I is defined by a tuple (S, M^S, Val^S, $\mathcal{H}$) where*

- *S = (N, D, NT, CtrlE, SyncE, ...) denotes WF schema the execution of I is based on.*
- *M^S = (NS^S, ES^S) describes node and edge markings of I:*
  NS^S: $N \mapsto$ {`NotActivated, Activated, Running, Completed, Skipped`}
  ES^S: $(CtrlE \cup SyncE \cup LoopE) \mapsto$ {`TrueSignaled, FalseSignaled`}
- *Val^S is a function on D. It reflects for each data element $d \in D$ either its current value or the value* `UNDEFINED` *(if d has not been written yet).*
- *$\mathcal{H} = < e_0, \ldots, e_k >$ is the execution history of I. $e_0, \ldots, e_k$ denote the start and end events of activity executions. For each started activity X the values of data elements read by X and for each completed activity Y the values of data elements written by Y are logged.*

3.2 Checking Compliance With Control Flow Changes

The ability to check compliance efficiently is indispensable for the flexible and efficient support of team ware processes by a WfMS. Regarding existing approaches, it remains pretty vague how compliance can be decided in conjunction with a multitude of running WF instances. Thus, we present formal and precise conditions for checking the logical compliance property (cf. Axiom 1) when new activities, control edges, or sync edges are inserted into a WF schema with related WF instance(s). (Note that the addition of a new activity node is always accompanied by the insertion of associated control or sync edges, which embed this activity into the WF schema context.) Due to a better structuring and understanding of this paper we focus on data flow issues later on (cf. Section 4).

Theorem 1 (Insertion of Activities/Control Edges/Sync Edges) *Let S = (N, D, NT, CtrlE, SyncE, LoopE, DP, EC) be a correct WF Schema and I be a WF instance on S with execution history $\mathcal{H}_{red}$. Assume further that change operation Δ transforms S into a correct WF schema S' = (N', D', NT', CtrlE', SyncE', LoopE', DP', EC').*

(a) Δ inserts an activity n_{insert} (with associated control and sync edges) into S. Then:

I is compliant with S' $\Leftrightarrow$
$\forall\ n \in \{x \in N \mid n_{insert} \rightarrow x \in (CtrlE' \cup SyncE')\}$:
NS(n) $\in$ {`NOT_ACTIVATED, ACTIVATED, SKIPPED`} $\vee$
n_{insert} is inserted into an already skipped branch of an XOR-branching

(b) Δ inserts a control edge $\mathtt{n}_{src} \rightarrow \mathtt{n}_{dest}$ into S. Then:

I is compliant with S' $\Leftrightarrow$ NS(n_{dest}) $\in$ {`NOT_ACTIVATED, ACTIVATED, SKIPPED`}

(c) Δ inserts a sync edge $\mathtt{n}_{src} \rightarrow \mathtt{n}_{dest}$ into S (n_{src} and n_{dest} ordered parallel so far). Then:

I is compliant with S' ⇔

$[NS(n_{dest}) \in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\}] \vee$
$[NS(n_{src}) = \texttt{COMPLETED} \wedge NS(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\}$ *with*
$\exists e_i = \texttt{END}(n_{src}),\ e_j = \texttt{START}(n_{dest}) \in \mathcal{H}_{red} \wedge i < j))] \vee$
$[NS(n_{src}) = \texttt{SKIPPED} \wedge NS(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\})$ *with*
$\forall\ n \in N_{critical}$ *with* $NS(n) \neq \texttt{SKIPPED}$*:*
$\exists e_i = \texttt{START}(\texttt{n}_{dest}),\ e_j = \texttt{END}(\texttt{n}) \in \mathcal{H}_{red}$ *with* $j < i$*),*
where $N_{critical} = (c\_pred^*(S, n_{src}) \neg c\_pred^*(S, n_{dest}))$
and $c\_pred^*(S, n))$ *denotes all direct/indirect predecessors of n in S concerning control edges*]

A formal proof of this Theorem is given in the Appendix. Informally, for adding activities, compliance can be always guaranteed if all (direct) successors of the newly inserted activity $\texttt{n}_{insert}$ are actually marked with ACTIVATED or NOT_ACTIVATED. In this case they have not yet written any entry into the execution history. Interestingly, the same applies when inserting activities into already skipped branches.

Concerning the insertion of a single control or sync edge, compliance can be always ensured if the target node of the respective edge has not been started yet. This is a sufficient condition for guaranteeing compliance, but it is not always necessary. In a few cases additional information from the reduced execution history may be required to ensure compliance. As an example take WF schema S from Fig. 2a. Assume that sync edge D → K is inserted into S. Regarding WF instance I (cf. Fig. 2b) we see that the source node D is skipped and the target node K is completed. According to Theorem 1c, in this situation, I is only compliant with the new schema iff B has written its end entry before the start entry of K into the execution history ($N_{critical} = \{\texttt{B}\} \wedge \text{NS}(\texttt{B}) \neq \texttt{SKIPPED}$). Considering the (execution) history from Fig. 2c, this constellation is obviously not given. Consequently, the insertion of sync edge D → K cannot be propagated to I.

Intuitively, delete operations are also very important for practical purposes, e.g., activities may have to be skipped (and therefore the associated control and sync edges embedding the respective activity into the workflow context be deleted). Thus we provide Theorem 2 which summarizes the compliance conditions for delete operations:

Theorem 2 (Deletion of Activities/Control Edges/Sync Edges) *Let S = (N, D, ...) be a correct WF Schema and I be a WF instance on S with execution history* $\mathcal{H}_{red}$*. Assume further that change operation* Δ *transforms S into a correct WF schema S' = (N', D', ...).*

(a) Δ *deletes an activity* n_{insert} *from S (including the re-linking of control edges). Then:*

I is compliant with S' ⇔ $NS(n_{delete}) \in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\}$

(b) Δ *deletes a control or sync edge* $\texttt{n}_{src} \rightarrow \texttt{n}_{dest}$ *from S. Then:*

I is compliant with S'

For delete operations compliance checks can be always performed solely on basis of activity markings. Intuitively, only those activities of a WF instance `I` can be dynamically deleted which have not yet written any entry into the execution history. This is the case if the node state of the activity to be deleted is `NOT_ACTIVATED, ACTIVATED`, or `SKIPPED`. Concerning control or sync edges their deletion is uncritical with respect to compliance of WF instances with the resulting WF schema. Note that order relations between the source and end activity nodes of deleted edges are abolished. Therefore the previous execution can be replayed on the changed schema.

Order changing operations are an example for complex change operations which can be simply built by serially applying one or more basic operations (i.e., insertion/deletion of control or sync edges). Fig. 3 shows such an order changing operation, namely swapping two activities `B` and `C`. The comprehensive compliance property can be always ensured in conjunction with such complex operations if the respective compliance conditions are fulfilled for each applied basic operation. Further optimizations are conceivable with respect to checking compliance for complex changes, but are outside the scope of this paper.

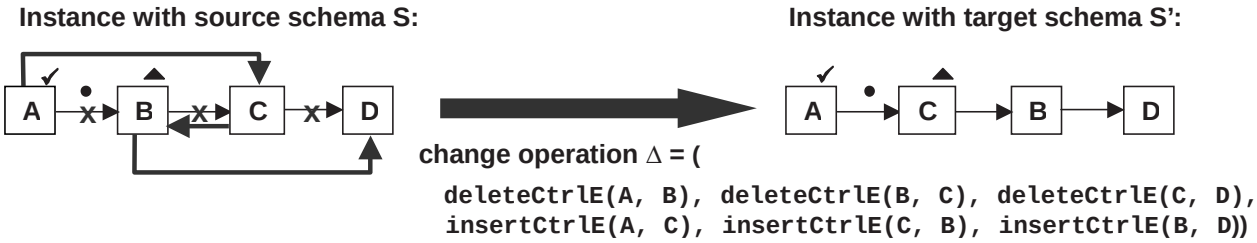


Figure 3: Complex Change Operation: Shifting An Activity

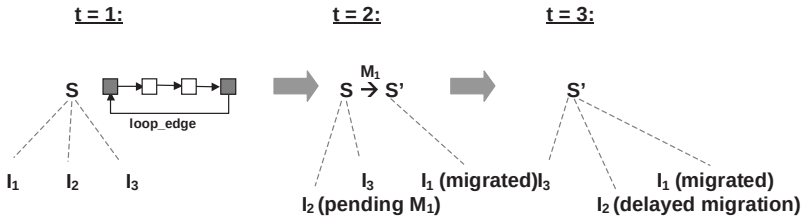
3.3 Never-More-Compliant and Re-Compliant WF Instances

Generally, applying the compliance property will lead to a set of WF instances, which do not fulfill this property and thus – at first glance – cannot be migrated. This includes WF instances, which can never be migrated (*"never-more-compliant instances"*) and others, which only fail because the current execution of a loop iteration has proceeded too far. The latter WF instances become a candidate for migration when the loop enters its next iteration (*"re-compliant instances"*).

Normally, *never-more-compliant instances* will never reach a state again in which they are compliant with the modified schema. The easiest way would be to finish these WF instances according to their old WF schema which requires appropriate versioning concepts [11, 13]. Alternatively, we can put these WF instances (or some of them) back to a compliant state by partial rollback [5, 21]. But on the one hand, only activities can be rolled back which support cancelation or compensation activities. On the other hand, rollback of processes is often out of touch with reality, in particular concerning teamware processes (e.g., patient treatment). Up to

now, only in [7] the authors have recognized that in the case of loop backs WF instances may become compliant with the changes WF schema again (*re-compliant instances*).

Re-compliant instances. In particular, the marking of a loop is reset if a loop back takes place such that Axiom 1 will be satisfied with delay. Thus, WF instances which are not compliant according to their actual loop iteration may become re-compliant when another loop iteration takes place and therefore can be migrated to the new schema with delay (*delayed migration*). As shown in the Fig. 4, re-compliant instances can be held as "pending to migration" until the loop condition is evaluated.



Event	Condition	Action
Loop_Back	ES(loop_edge) = TRUE_SIGNALED	migrate I_2 to S'

Figure 4: Principle Of Delayed Migration

The treatment of re-compliant instances, which is especially important in conjuntion with long-running processes, is not as trivial as it looks like at first glance. At first, if an instance contains nested loops there can be several events (loop backs) to trigger the execution of a previously delayed migration. Furthermore, the interesting question remains how to deal with pending instances if further schema changes take place. Due to lack of space we abstain from further discussion of this point.

4 Checking Compliance With Data Flow Changes

As outlined in the introduction, the proper handling of data flows and data flow changes is essential for WfMS, which shall be broadly applicable. However, data flow changes and their influence on running WF instances have been totally factored out by existing approaches so far. In particular, in some approaches (e.g., WF models based in Petri Nets), the flow of data can be only modeled in an implicit way or mixed with control flow specification. Doing so aggravates any check of compliance in conjunction with data flow changes.

In the sequel, we discuss how Axiom 1 can be ensured in conjunction with data flow changes. To provide a basis for discussion, we first discuss some details about the modeling of data flows in ADEPT.

4.1 Data Flow Basics in ADEPT

The *data flow* between activities is modeled by connecting *input/output parameters* of WF activities with global variables (*data elements*). Thereby each activity *input parameter* is mapped to exactly one data element by a *read data edge* and each activity *output parameter* is connected to a data element by a *write data edge*. An example is shown in Fig. 2a. Activity A writes *data element* $\mathtt{d}_1$ which is then read by activity `B`. For the modeling of such a data flow schema (*DF schema*) a number of correctness properties must be met. The most important one is that for each activity the data flow ensures that all mandatory input parameters will be supplied at runtime (i.e., no bad surprises will occur when invoking activity programs).

At runtime, different versions of a data object may be stored for a data element. For each write access, always a new version is created, i.e., data objects are not physically overwritten. Holding different versions is important for the context-dependent reading of data elements as well as for rollback operations in case of failures. To simplify matters, we assume that the data element values are logged within the execution history, i.e., for each started activity X the values of the data objects read by X and for each completed activity Y the values of the data objects written by Y are stored together with the respective history entry (cf. Fig. 2c).

4.2 Checking Compliance for Data Flow Changes

Changes of a DF schema may become necessary in conjunction with control flow schema changes (e.g., removing associated data edges of an activity to be deleted) or may have to be applied independently in order to re-link data edges or data elements (e.g., if errors in the modeled data flow have to be corrected). To modify DF schemes, ADEPT offers operations for adding and deleting data elements as well as data edges.

Taking the compliance property from Axiom 1, all conditions set out for control flow changes (cf. Theorem 1 and 2) must be further fulfilled. Additionally it is required that each started or finished activity (of the respective WF instance) would have read and each finished activity would have written the same data element values also on the new schema. The compliance of a WF instance in case of DF schema changes can be easily checked based on the folowing conditions.

Theorem 3 (Data Flow Changes) *Let S = (N, D, ...) be a correct WF Schema with DF schema DFS and let I be a WF instance on S with execution history* $\mathcal{H}_{red}$*. Assume that* Δ *transforms S into a correct WF schema S' = (N', D', ...) with DF schema DFS'.*

(a) Δ *inserts a data element d into DFS. Then I is compliant with S'.*

(b) Δ *deletes a data element d from DFS. Then:*

I is compliant with S' $\Leftrightarrow$

No read or write access by an activity with state `RUNNING` *or* `COMPLETED`

(c) Δ *inserts or deletes a read edge* $d \rightarrow n$*. Then:*

I is compliant with S' ⇔ NS(n) $\in$ {`NOT_ACTIVATED, ACTIVATED, SKIPPED`}

(d) Δ *inserts or deletes a write edge* $n \rightarrow d$*. Then:*

I is compliant with S' ⇔ NS(n) $\neq$ `COMPLETED`

As already mentioned, data flow adaptations also become necessary in conjunction with the insertion and deletion of activities. In this case, the conditions of Theorem 3 are already met if the state conditions of the according node insertion or deletion operations are fulfilled (cf. Theorem 1 and 2). Concerning data flow changes, again the conditions for using complex operations arise from the aggregation of the conditions of basic change operations.

5 Further Issues and Proof-Of-Concept Prototype

The results presented in this paper are embedded in a major project on adaptive WF management [17, 18]. We do not only focus on efficiently checking compliance of running WF instance with a changed WF schema but work on further important issues related to evolutionary processes as well. The first important question is how to adapt WF instance markings after their migration to the changed WF schema. In [19] we present an efficient algorithm for these marking adaptations with linear complexity.

Especially important for team-oriented processes is the interplay of WF schema modification (and their propagation to a potentially large collection of in-progress WF instances) and ad-hoc changes of single WF instances. Think of, for example, team processes where the related WF schema has to be adapted to a new law, but single WF instances have already been changed by team members (e.g., due to exceptional situations). The challenging question, arising in this context, is whether the WF schema changes can be correctly propagated to the individually modified WF instances as well and how to efficiently check this [12]. Intuitively, checking compliance no longer depends just on state conditions for individually modified instances. Moreover, structural and semantical conflicts between the WF schema and the WF instance change have to be taken into account as well [20, 19].

We have implemented the presented results in a powerful proof-of-concept prototype. Some illustrative screens of the WfMS are shown in Fig. 5 and 6. In Fig. 5, we start with the WF schema `medical treatment` in its first version `V1`. Fig. 5 also shows two related WF instances `Instance 1` and `Instance 2` (out of altogether 2000 WF instances running according to the schema `medical treatment, V1`) and the execution history of `Instance 2`.

Our prototype includes a WF editor which allows to create new WF schemes and to correctly change existing ones. Each time a modified WF schema is released, a new schema version

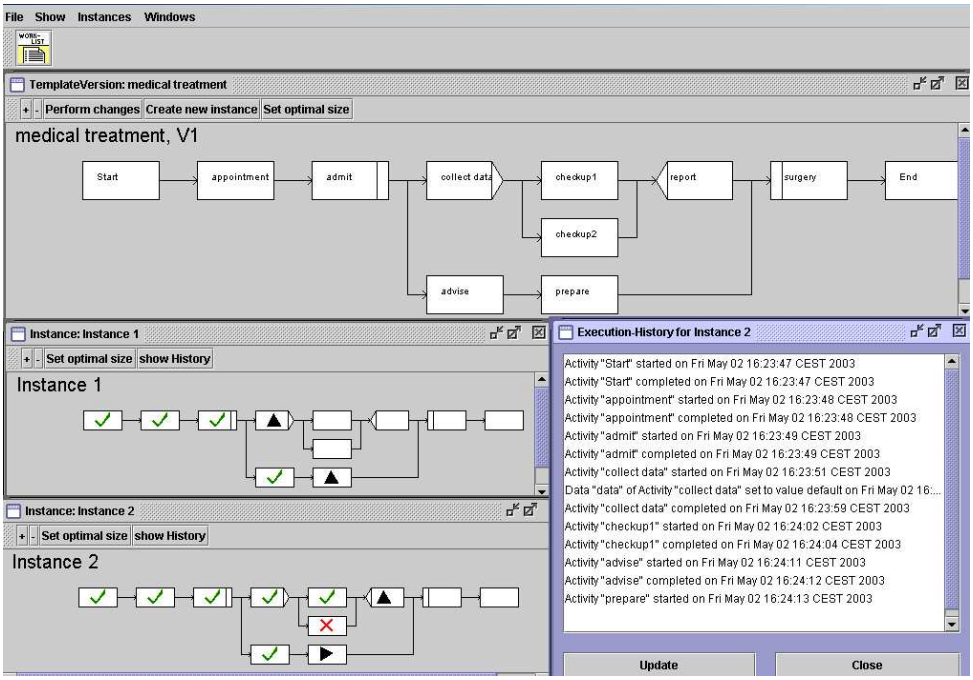


Figure 5: Example For A Medical Treatment: Pre-Change

is generated and stored in the repository. Additionally, if the user wants the system to do so, compliance is checked for all running WF instances based on the old WF schema so far. Afterwards, all compliant instances are migrated to the new WF schema version by correctly adapting their markings and related data structures (e.g., user worklists). The results of such a migration process are summarized in a `Migration Report` (see Fig. 6 for an example). Fig. 6 shows the WF schema version `V2` resulting from a change of the WF schema `medical treatment (V1)` depicted in Fig. 5, namely the insertion of a new activity `diabetes test`. Fig. 6 also shows the two instances from Fig. 5 after change propagation: `Instance 1` has been compliant with WF schema version `V2` and has therefore been migrated to `V2`, whereas `Instance 2` remains unchanged since it is not compliant with `V2` (cf. Fig. 6).

From the `Migration Report` shown in Fig. 6 it can be seen that the necessary compliance checks only took a very little fraction of time (when compared to the approaches replaying the whole execution history). Therefore, implementing this proof-of-concept prototype affirms that the proposed compliance checks (cf. Theorems 1 and 2) are very quick for complex WF graphs as well as for a large number of active instances. As mentioned above the set of WF instances for which compliance has to be decided can be shrunken by user defined constraints (e.g., "migrate only those WF instances that have been started after Dec, 31th 2002").

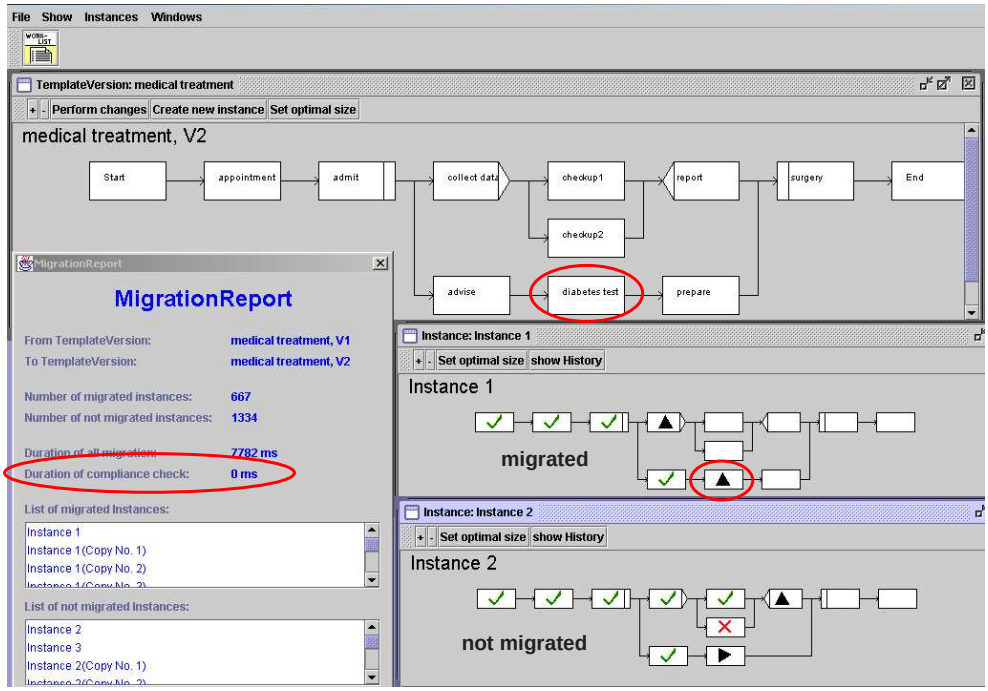


Figure 6: Example For A Medical Treatment: Post-Change

6 Related Work

Obviously, there are similarities between schema changes in WfMS [5, 20, 21, 23] and in DBMS [2]. The underlying problems are similar if considerations are restricted to the mapping of schema elements (activity nodes, control/data flow edges) from the old to the new schema. WF schema evolution, however, also raises orthogonal issues. If changes at the WF schema level shall be applied at the WF instance level as well, one has to consider that WF instances may be in a different state when a change propagation takes place. Depending on their current state and on the applied change operations, a migration to the new schema may then be possible or not. For deciding which instances are compliant with the new schema and which can therefore be smoothly migrated to it, theoretically sound and efficient solutions are required.

Regarding related work on WF schema evolution [5, 20, 21, 23, 7, 9], we distinguish between *history* and *snapshot based approaches*. The latter only consider currently activated or running activities without maintaining information about their previous execution (e.g., Petri Nets).

History Based Approaches. WIDE [5] offers a complete and minimal set of basic operations to transform a correct schema S into another correct schema S'. To migrate WF instances to S', for the first time, the (naive) compliance property as discussed in Section 2 has been suggested. TRAM [13] focuses on WF schema versioning concepts. To efficiently manage an instance

migration the authors propose the definition of so called migration conditions for each change operation. With these conditions it can be decided whether an instance can smoothly migrate to the new WF schema version or not. Recent results concerning WF schema evolution come from the BREEZE project [21], which uses a model and change operations similar to our ADEPT approach [17]. BREEZE uses compliance as a correctness criterion as well but focuses on the question how to deal with non-compliant WF instances. In summary, all these approaches are too restrictive in conjunction with loops since they are based on the (naive) compliance property. Furthermore, compliance in connection with data flow schema changes has not been considered in detail. Finally, the authors do not show how their suggested compliance property can be (formally) checked, which is important when incorporating compliance checks into a WF engine implementation.

Object oriented approaches are offered by [11, 25]. In MOKASSIN [11] changes are carried out by encapsulating change primitives within WF instances. Consequently, WF instances or users are themselves responsible for preserving consistency. The (naive) compliance property is considered as being too restrictive. Instead, a more granular version concept is proposed, but without discussing issues related to (efficient) compliance checks. Another versioning approach has been presented by WASA_2 [25], which proposes a mapping between the modified WF schema and the sub-workflows resulting from the corresponding instances to allow efficient compliance checks. However, data flow changes have not been treated in detail and formal considerations are not given.

Snapshot Based Approaches. Petri Net based approaches [7, 8, 22, 23] fight with several approach-inherent problems: Generally, they often lack a clear seperation between control and data flow tokens, which complicates (dynamic) net changes. In [7], both, the WF schema and the WF instances are captured in one Petri net based on coloured markings. (To avoid misunderstandings, in our approach, multiple WF instances may be related to the same WF schema. As opposed to Petri Nets, however, each WF instance has its own marking defined on that schema.) A schema modification is carried out by substituting marked sub nets, whereas precise or formal conditions for checking compliance of WF instances with the new net are missing. Another serious problem arises from the fact that markings of previously passed regions are not preserved and "skipped" regions are not marked at all. Therefore the "challenging" question is how to adapt instance markings after propagating a schema change without knowledge of their previous execution. In [8] the WF designer has to manually adapt the markings for each WF instance. What adds insult to injury is that complex reachability analyses become necessary to check consistency of net markings after a change. In contrast, the compliance conditions proposed in this paper and the respective marking adaptation algorithms (cf. [19]) are of linear complexity. Recent approaches wrestle with that problem as well. In [22] the authors propose that WF schema modifications shall not be propagated to WF instances which are executed on modified regions. The adaptation of markings is seen as a very complex problem (the so called dynamic change bug) [23]. To fix this bug the authors suggest that the modeler has to specify a mapping between the markings of the old net an the new net which has to be applicable for every running instance [23]. Besides, Petri Nets suffer from the implicit modeling of cycles. Thus the distinction between desired cycles and deadlocks is a NP-hard problem.

7 Summary and Outlook

Applications which aim at the support of complex, long-running team processes need adaptive workflow to be able to react rapidly to process changes. Thus, the support of WF schema evolution in connection with sound and simple compliance checks (as described in this paper) is an indispensable feature of any WfMS. In this paper we have elaborated a comprehensive and formal foundation for checking compliance of WF instances with a (modified) WF schema. The compliance criteria embrace WF schemes with (nested) loops and with explicitly defined data flows. Theses criteria come along with efficient check algorithms and thus provide a proper basis for the implementation of these features in a WfMS. The solution has been described using the ADEPT model but may be easily applied to other WF models with similar properties (e.g. [3, 15]).

In this paper we have concentrated on correctness criteria and their efficient evaluation in the context of WF schema evolution. How to efficiently check WF instances for compliance is one issue, how to "physically" perform the migrations (incl. correct state adaptations), how to internally represent WF instances and WF schemes, how to interact with the WF schema designer (who defines the change) or how to adapt user worklists, how to to deal with concurrent changes (and with locking issues in this context) are other important questions. Work on some of these issues is in progress [20, 19]. The challenge is to elaborate solutions, which do not work only in an isolated fashion but in conjunction with each other.

References

[1] A. Agostini and G. De Michelis. A light workflow management system using simple process models. *Computer Supported Cooperative Work: The Journal of Collaborative Computing*, 9(3-4):335–363, August 2000.

[2] J. Andany, M. Leonard, and C. Palisser. Management of schema evolution in databases. In *Proc. Int'l Conf. on Very Large Databases*, pages 161–170, Barcelona, September 1991.

[3] S. Bassil, M. Benyoucef, R. Keller, and P. Kropf. Addressing dynamism in e-negotiations by workflow management systems. In *Proc. DEXA'2002 Workshop*, September 2002.

[4] T. Bauer and P. Dadam. Efficient distributed workflow management based on variable server assignments. In *Proc. CAiSE '00*, pages 94–109, Stockholm, June 2000.

[5] F. Casati, S. Ceri, B. Pernici, and G. Pozzi. Workflow evolution. *Data and Knowledge Engineering*, 24(3):211–238, 1998.

[6] F. Curbera, Y. Goland, J. Klein, F. Leymann, D. Roller, S. Thatte, and S. Weerawarana. *Business Process Execution Language for Web Services, Version 1.0*, 2002. http://www.ibm.com/developerworks/library/ws-bpel/.

[7] C.A. Ellis, K. Keddara, and G. Rozenberg. Dynamic change within workflow systems. In *Proc. Int'l ACM Conf. on Organizational Comp. Sys. (COOCS '95)*, pages 10–21, Milpitas, CA, August 1995.

[8] C.A. Ellis and C. Maltzahn. The Chautauqua workflow system. In *Proc. 30th Int'l Conf. on System Science*, Maui, 1997.

[9] A. Fent, H. Reiter, and B. Freitag. Design for change: Evolving workflow specifications in ULTRAflow. In *Proc. Int'l Conf. on Advanced Information Systems Engineering (CAISE '02)*, pages 516–534, May 2002.

[10] C. Hensinger, M. Reichert, T. Bauer, T. Strzeletz, and P. Dadam. ADEPT$_{workflow}$ - advanced workflow technology for the efficient support of adaptive, enterprise-wide processes. In *Proc. Software Demonstration Track (EDBT '00)*, Konstanz, March 2000.

[11] G. Joeris and O. Herzog. Managing evolving workflow specifications. In *Proc. Int'l Conf. on Cooperative Information Systems (CoopIS '98)*, pages 310–321, New York City, August 1998.

[12] K. Kochut, J. Arnold, A. Sheth, J. Miller, E. Kraemer, B. Arpinar, and J. Cardoso. IntelliGEN: A distributed workflow system for discovering protein-protein interactions. *Distributed and Parallel Databases*, 13:43–72, 2003.

[13] M. Kradolfer and A. Geppert. Dynamic workflow schema evolution based on workflow type versioning and workflow migration. In *Proc. CoopIS '99*, pages 104–114, Edinburgh, September 1999.

[14] F. Leymann and D. Roller. *Production Workflow.* Prentice Hall, 2000.

[15] R. Müller and E. Rahm. Dealing with logical failures for collaborating workflows. In *Proc. Int'l 5th Conf. on Cooperative Information Systems*, pages 210–223, Eilat, 2000.

[16] P. Muth, J. Weissenfels, M. Gillmann, and G. Weikum. Workflow history management in virtual enterprises using a light-weight workflow management system. In *Proc. RIDE'99*, March 1999.

[17] M. Reichert and P. Dadam. ADEPT$_{flex}$ - supporting dynamic changes of workflows without losing control. *Journal of Intelligent Information Systems*, 10(2):93–129, 1998.

[18] M. Reichert, S. Rinderle, and P. Dadam. ADEPT workflow management system: Flexible support for enterprise-wide business processes (tool presentation). In *Int'l Conf. on Business Process Management (BPM '03)*, Eindhoven, The Netherlands, June 2003. (to appear).

[19] M. Reichert, S. Rinderle, and P. Dadam. A formal framework for workflow type and instance changes under correctness constraints. Technical Report UIB-2003-01, University of Ulm, Computer Science Faculty, April 2003.

[20] S. Rinderle, M. Reichert, and P. Dadam. Evaluation of correctness criteria for dynamic workflow changes. In *Int'l Conf. on Business Process Management (BPM '03)*, Eindhoven, The Netherlands, June 2003. (to appear).

[21] S. Sadiq, O. Marjanovic, and M. Orlowska. Managing change and time in dynamic workflow processes. *The International Journal of Cooperative Information Systems*, 9(1&2), 2000.

[22] W.M.P. van der Aalst. Exterminating the dynamic change bug: A concrete approach to support worfklow change. *Information Systems Frontiers*, 3(3):297–317, 2001.

[23] W.M.P van der Aalst and T. Basten. Inheritance of workflows: An approach to tackling problems related to change. *Theoretical Computer Science*, 270(1-2):125–203, 2002.

[24] M. Weber. *Distributed Systems.* Spektrum, Akademischer Verlag, 1998. (in German).

[25] M. Weske. Flexible modeling and execution of workflow activities. In *Proc. 31st Int'l Conf. on System Sciences*, pages 713–722, Hawaii, 1998.

Appendix

Proof of Theorem 1

To prove Theorem 1 we first give some useful information. To begin with, we do not need any special treatment of loops since using the reduced execution history logically leads to a "loop-free" WF schema. Thus we have to care about acyclic WF schema graphs with sequences, AND-branchings and XOR-branchings. Furthermore, Table 2 informally summarizes certain predecessor and successor functions on WF schema graphs which are needed for the following considerations.

c_succ(S,n) / c_pred(S,n)	set of all *direct* successors / predecessors of activity n considering only edges e ∈ CtrlE in WF schema S
c_succ*(S,n) / c_pred*(S,n)	set of all *direct* or *indirect* successors / predecessors of activity n considering only edges e ∈ CtrlE in WF schema S
succ(S,n) / pred(S,n)	set of all *direct* successors / predecessors of activity n referring to edges e ∈ (CtrlE ∪ SyncE) in WF schema S
succ*(S,n) / pred*(S,n)	set of all *direct* and *indirect* successors / predecessors of activity n referring to edges e ∈ (CtrlE ∪ SyncE) in WF schema S succ*(S,n) = {n* ∈ N | n* ∈ succ(S,n) ∨ (∃ n** ∈ succ(S,n): n* ∈ succ*(S,n**))}

Table 2: Predecessor and Successor Functions on WF Graphs

Finally, we need the following Lemma 1 to prove Theorem 1. It states that all predecessors of a running or completed activity n^* must have one of the markings COMPLETED or SKIPPED.

Lemma 1 *Let S=(N, D, ...) be a correct WF schema and I a WF instance on S. Then:*

$\forall\ n^* \in N$ *with NS(*n^**)* $\in$ {RUNNING, COMPLETED, SKIPPED} $\Rightarrow$

$\forall n \in$ pred*(*S, n^**): NS(n)* $\in$ {COMPLETED, SKIPPED}

Proof Sketch (Lemma 1)
For arbitrary paths w = $i_0 \rightarrow \ldots \rightarrow i_k$ in S we can show by induction over the length k of w:

$[\text{NS}(i_k) \in \{\texttt{RUNNING, COMPLETED, SKIPPED}\} \Rightarrow \text{NS}(i_\mu) \in \{\texttt{COMPLETED, SKIPPED}\}\ \forall \mu = 0, \ldots, k-1]$

Based on this, the proposition of Lemma 1 can be easily proven.

We now have done all necessary prepartory work for proving Theorem 1.

Proof (Theorem 1):

(a) Δ inserts an activity n_{insert} (with associated control and sync edges) into S.

This proposition can be more formally described as follows:
I is compliant with S' $\Leftrightarrow B_1 \vee B_2 \vee B_3$ with
$B_1 \equiv [\forall n \in \texttt{succ(S',}n_{insert}\texttt{)}$: NS(n) $\in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\}]$
$B_2 \equiv [\forall$ n $\in \texttt{c\_pred(S', }n_{insert}\texttt{)}$: NS(n) = SKIPPED]
$B_3 \equiv [n_{insert}$ is inserted into a skipped, empty branch]

(The statement "n_{insert} is inserted into an already skipped branch" corresponds to $B_2 \vee B_3 \vee$ $[\forall n \in \texttt{c\_succ(S',}n_{insert}\texttt{)}$: NS(n) = SKIPPED]
where the last term is already included by B_1.)

"$\Rightarrow$" I is compliant with S' $\Rightarrow B_1 \vee B_2 \vee B_3$
Proof by Contradiction, we show: $\neg(B_1 \vee B_2 \vee B_3) \Rightarrow$ I is not compliant with S'

Assumption: $\neg(B_1 \vee B_2 \vee B_3)$ holds
$\neg(B_1 \vee B_2 \vee B_3) \equiv \neg B_1 \wedge \neg B_2 \wedge \neg B_3$
$\equiv [\exists n^* \in \texttt{succ}$(S', n_{insert}): NS(n^*) $\in \{\texttt{RUNNING, COMPLETED}\} \wedge$
$[\exists n^{**} \in$ c_pred(S', n_{insert}): NS(n^{**}) $\neq$ SKIPPED] $\wedge$
$[n_{insert}$ is not inserted into a skipped, empty branch]
With $\neg B_1$ and Lemma 1 we obtain NS'(n_{insert}) $\in \{\texttt{COMPLETED, SKIPPED}\}$. Consequently, the marking NS(n_{insert}) must be SKIPPED. After re-evaluating the marking of the modified instance (cf. Fig. 2e), a newly inserted activity will be either marked as SKIPPED (insertion into a skipped branch) or as NOT_ACTIVATED or ACTIVATED.

Taking the above assumption, n_{insert} must therefore have been inserted into an already skipped branch of an XOR-branching with split node s and join node j. Because of $\neg B_3$ this branch cannot be empty. Based on this, it either follows that n_{insert} is not a direct successor of s – then $\forall$ n $\in$ c_pred(S', n_{insert}): NS(n) = SKIPPED – or n_{insert} is not a direct predecessor of j – $\forall$ n $\in$ c_succ(S', n_{insert}): NS(n) = SKIPPED. The first statement can not be true because of $\neg B_2$ and the latter because of $\neg B_1$. This is contradicting to our assumption. □

Let now statements C_1 and C_2 be as follows:
$C_1 \equiv [\forall$ n $\in \texttt{succ(S',}n_{insert}\texttt{)}$: NS(n) $\in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\}]$
$C_2 \equiv [n_{insert}$ is inserted into a skipped branch of an XOR-branching]

"$\Leftarrow$": $C_1 \vee C_2 \Rightarrow$ I is compliant with S' (according to Axiom 1)

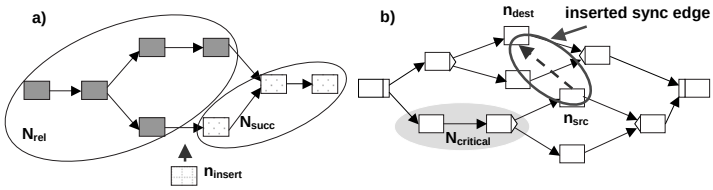


Figure 7: Important Sets of a WF Schema Referring to n_{insert}

We first prove $C_1 \Rightarrow$ I is compliant with S'.
Assumption:

$C_1 \equiv [\forall$ n $\in$ `succ(S',`n_{insert}`)`: NS(n) $\in$ {`NOT_ACTIVATED, ACTIVATED, SKIPPED`}]
$\Rightarrow \forall$ n $\in$ `succ(S',`n_{insert}`)`: $\nexists\ e_i \in \mathcal{H}_{red}$ with $e_i \in$ {`START(n), END(n)`}
$\Rightarrow \forall$ n $\in$ `succ`*`(S',`n_{insert}`)`: $\nexists\ e_i \in \mathcal{H}_{red}$ with $e_i \in$ {`START(n), END(n)`} ($\diamond$)

That means that the history $\mathcal{H}_{red}$ contains no entry of a direct or indirect successor of n_{insert}. Furthermore, a re-evaluation of the instance marking results in

NS'(n_{insert}) $\in$ {`NOT_ACTIVATED, ACTIVATED, SKIPPED`}
$\Rightarrow \nexists\ e_i \in \mathcal{H}_{red}$ with $e_i \in$ {`START(`n_{insert}`), END(`n_{insert}`)`} ($\diamond\diamond$)

We now show that I is compliant with S', i.e., the previous execution events $e_0, \ldots, e_k$ stored in $\mathcal{H}_{red}$ can be applied to S' in the given order.

Let N_{rel} be the set of all activity nodes of N' which can be executed before n_{insert} is started(see Fig. 7a). So, N_{rel} contains all activity nodes positioned before or parallel to n_{insert}. Formally:

N_{rel} := pred*(S', n_{insert}) $\cup$ {n $\in$ N' | n $\notin$ pred* (S', n_{insert}) $\wedge$ n $\notin$ succ*(S', n_{insert})}

With ($\diamond$) and ($\diamond\diamond$) it follows:

$\forall\ e_i \in \mathcal{H}_{red}$ with $e_i =$ `START(n)` $\vee\ e_i =$ `END(n)`: n $\in N_{rel} \subseteq$ N

Thus all entries of $\mathcal{H}_{red}$ have been written by activity nodes which are – in principle – executable before n_{insert} referring to S'. Since the subgraph of S induced by the node set N_{rel} (cf. Fig. 7a) is not affected by the insertion and therefore remains unchanged, $e_1, \ldots, e_k$ can be carried out on this subgraph in the given order and therefore on S' as well.
Referring to the second part [$C_2 \Rightarrow$ I is compliant with S'] it is clear that n_{insert} is inserted into a skipped branch, i.e., we obtain NS'(n_{insert}) = `SKIPPED`. Therefore n_{insert} has not yet written any entry into the execution history. Consequently, the previous execution history $\mathcal{H}_{red}$ is producible on S' as well. □

In the following, we first prove part (c) of Theorem 1 (insertion of sync edges into S) since part (b) (insertion of control edges) is less complex and can be proven in a similar way.

(c) Δ inserts a sync edge $\mathtt{n}_{src} \rightarrow \mathtt{n}_{dest}$ into S (n_{src} and n_{dest} ordered parallel so far).

First let
$A_1 \equiv$ [NS(n_{dest}) $\in$ {`NOT_ACTIVATED, ACTIVATED, SKIPPED`}]

$A_2 \equiv [(\text{NS}(n_{src}) = \texttt{COMPLETED} \wedge \text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\})$ with
$\exists e_i, e_j \in \mathcal{H}_{red}$: $i < j \wedge e_i = \texttt{END}(n_{src})$, $e_j = \texttt{START}(n_{dest})]$
$A_3 \equiv [(\text{NS}(n_{src}) = \texttt{SKIPPED} \wedge \text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\})$ with
$\forall n \in N_{critical}$ with NS(n) $\neq$ SKIPPED:
$\exists e_k, e_l \in \mathcal{H}_{red}$: $l < k \wedge e_k = \texttt{START}(n_{dest})$, $e_l = \texttt{END(n)}]$
where $N_{critical} = (\text{c\_pred}^*(n_{src}) \neg \text{c\_pred}^*(n_{dest}))$ (cf. Fig. 7b)

The negation of A_1, A_2 and A_3 yields
$\neg A_1 \equiv [\text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\}]$
$\neg A_2 \equiv [\text{NS}(n_{src}) \neq \texttt{COMPLETED} \vee \text{NS}(n_{dest}) \in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\} \vee$
$\nexists e_i, e_j \in \mathcal{H}_{red}$: $i < j \wedge e_i = \texttt{END}(n_{src})$, $e_j = \texttt{START}(n_{dest})]$
$\neg A_3 \equiv [\text{NS}(n_{src}) \neq \texttt{SKIPPED} \vee \text{NS}(n_{dest}) \in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\} \vee$
$\exists n \in N_{critical}$ with NS(n) $\neq$ SKIPPED:
$\nexists e_k, e_l \in \mathcal{H}_{red}$: $l < k \wedge e_k = \texttt{START}(n_{dest})$, $e_l = \texttt{END(n)}]$

"⇒": I is compliant with S' $\Rightarrow A_1 \vee A_2 \vee A_3$
Proof by contradiction, we show: $\neg(A_1 \vee A_2 \vee A_3) \Rightarrow$ I is not compliant with S'
Assumption: $\neg(A_1 \vee A_2 \vee A_3)$ holds.

$\neg(A_1 \vee A_2 \vee A_3) \equiv \neg A_1 \wedge \neg A_2 \wedge \neg A_3 \equiv (\neg A_1 \wedge \neg A_2) \wedge \neg A_3$
$\equiv [(\text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\} \wedge \text{NS}(n_{src}) \neq \texttt{COMPLETED}) \vee$
$\text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\} \wedge$
$\nexists e_i, e_j \in \mathcal{H}_{red}$: $i < j \wedge e_i = \texttt{END}(n_{src})$, $e_j = \texttt{START}(n_{dest}))] \wedge \neg A_3$
$\equiv [(\text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\} \wedge \text{NS}(n_{src}) \neq \texttt{COMPLETED}) \vee$
$((\exists e_j \in \mathcal{H}_{red}$: $e_j = \texttt{START}(n_{dest}))) \wedge$
$((\nexists e_i \in \mathcal{H}_{red}$: $e_i = \texttt{END}(n_{src})) \vee (\exists e_i \in \mathcal{H}_{red}$: $e_i = \texttt{END}(n_{src}) \wedge i > j)))] \wedge \neg A_3$
$\equiv [(\text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\} \wedge \text{NS}(n_{src}) \neq \texttt{COMPLETED}) \vee$
$((\exists e_j \in \mathcal{H}_{red}$: $e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}$: $e_i = \texttt{END}(n_{src})) \vee$
$(\exists e_i, e_j \in \mathcal{H}_{red}$: $e_j = \texttt{START}(n_{dest})$, $e_i = \texttt{END}(n_{src}) \wedge i > j))] \wedge \neg A_3$
$\equiv [(\exists e_j \in \mathcal{H}_{red}$: $e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}$: $e_i = \texttt{END}(n_{src})) \vee$
$(\exists e_i, e_j \in \mathcal{H}_{red}$: $e_j = \texttt{START}(n_{dest})$, $e_i = \texttt{END}(n_{src}) \wedge i > j)] \wedge \neg A_3$
$\equiv: (E_1 \vee E_2) \wedge \neg A_3$ $(\equiv (E_1 \wedge \neg A_3) \vee (E_2 \wedge \neg A_3))$

Because of $n_{src} \in$ pred(S', n_{dest}) and due to the compliance of I with S' the end entry of n_{src} cannot be situated before the start entry of n_{dest} in the execution history $\mathcal{H}_{red}$; i.e., E_2 and therefore $(E_2 \wedge \neg A_3)$ cannot hold. Accordingly, $(E_1 \wedge \neg A_3)$ must hold.

$(E_1 \wedge \neg A_3)$
$\equiv [\exists e_j \in \mathcal{H}_{red}$: $e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}$: $e_i = \texttt{END}(n_{src})] \wedge$
$[\text{NS}(n_{src}) \neq \texttt{SKIPPED} \vee \text{NS}(n_{dest}) \in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\} \vee$
$\exists n \in N_{critical}$, NS(n) $\neq$ SKIPPED:
$\nexists\ e_k, e_l \in \mathcal{H}_{red}$: $l < k \wedge e_k = \texttt{START}(n_{dest})$, $e_l = \texttt{END(n)}]$
$\equiv [\exists e_j \in \mathcal{H}_{red} : e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}$: $e_i = \texttt{END}(n_{src}) \wedge \text{NS}(n_{src}) \neq \texttt{SKIPPED}]$
$\vee [(\exists e_j \in \mathcal{H}_{red}$: $e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}$: $e_i = \texttt{END}(n_{src})) \wedge$

$\text{NS}(n_{dest}) \in \{\texttt{NOT\_ACTIVATED, ACTIVATED, SKIPPED}\}) \vee$
$(\exists e_j \in \mathcal{H}_{red}\text{: } e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}\text{: } e_i = \texttt{END}(n_{src}) \wedge$
$(\exists n \in N_{critical}, \text{NS(n)} \neq \texttt{SKIPPED}\text{:}$
$\nexists\ e_k, e_l \in \mathcal{H}_{red}\text{: } l < k \wedge e_k = \texttt{START}(n_{dest}), e_l = \texttt{END(n)}))]$
$\equiv [\exists e_j \in \mathcal{H}_{red}\text{: } e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}\text{: } e_i = \texttt{END}(n_{src}) \wedge \text{NS}(n_{src}) \neq \texttt{SKIPPED}]$
$\vee[(\exists e_j \in \mathcal{H}_{red}\text{: } e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}\text{: } e_i = \texttt{END}(n_{src}) \wedge$
$(\exists n \in N_{critical}, \text{NS(n)} \neq \texttt{SKIPPED}\text{:}$
$\nexists\ e_k, e_l \in \mathcal{H}_{red}\text{: } l < k \wedge e_k = \texttt{START}(n_{dest}), e_l = \texttt{END(n)}))]$
$\equiv\text{: } C_1 \vee C_2$

C_1 results in $\text{NS}(n_{dest}) \in \{\texttt{RUNNING, COMPLETED}\} \wedge \text{NS}(n_{src}) \notin \{\texttt{COMPLETED, SKIPPED}\}$. In this case I cannot be compliant with S'. Therefore C_2 must hold.

C_2
$\equiv[\exists e_j \in \mathcal{H}_{red}\text{: } e_j = \texttt{START}(n_{dest}), \nexists e_i \in \mathcal{H}_{red}\text{: } e_i = \texttt{END}(n_{src}) \wedge$
$(\exists n \in N_{critical}$ with $\text{NS(n)} \neq \texttt{SKIPPED}\text{:}$
$\nexists\ e_k, e_l \in \mathcal{H}_{red}\text{: } l < k \wedge 7\ e_k = \texttt{START}(n_{dest}), e_l = \texttt{END(n)})]$
$\equiv (\exists e_j \in \mathcal{H}_{red}\text{: } e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}\text{: } e_i = \texttt{END}(n_{src})) \wedge$
$(\exists n \in N_{critical}, \text{NS(n)} \neq \texttt{SKIPPED} \wedge$
$(\nexists e_l \in \mathcal{H}_{red}\text{: } e_l = \texttt{END(n)} \vee \exists e_l \in \mathcal{H}_{red}\text{: } e_l = \texttt{END(n)} \wedge j < l\ ))$
$\equiv [(\exists e_j \in \mathcal{H}_{red}\text{: } e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}\text{: } e_i = \texttt{END}(n_{src})) \wedge$
$(\exists n \in N_{critical}, \text{NS(n)} \neq \texttt{SKIPPED} \wedge \nexists e_l \in \mathcal{H}_{red}\text{: } e_l = \texttt{END(n)})] \vee$
$[(\exists e_j \in \mathcal{H}_{red}\text{: } e_j = \texttt{START}(n_{dest}) \wedge \nexists e_i \in \mathcal{H}_{red}\text{: } e_i = \texttt{END}(n_{src})) \wedge$
$(\exists n \in N_{critical}, \text{NS(n)} \neq \texttt{SKIPPED} \wedge \exists e_l \in \mathcal{H}_{red}\text{: } e_l = \texttt{END(n)} \wedge j < l\ )]$
$\equiv\text{: } D_1 \vee D_2$

Because of D_1 it follows that there is a predecessor node $\text{n} \in N_{critical}$ of n_{src} which is neither marked as COMPLETED nor as SKIPPED (see Fig. 7b). Referring to S' this node is also a predecessor of n_{dest} since S' contains the additional edge $n_{src} \rightarrow n_{dest}$. Accordingly, I cannot be compliant with S'.
D_2 yields that a predecessor node $\text{n} \in N_{critical}$ of n_{src} with $\text{NS(n)} = \texttt{COMPLETED}$ exists whose end entry is situated after the start entry of n_{dest} in the execution history $\mathcal{H}_{red}$. Since n is a predecessor of n_{dest} in S' it follows that I is not compliant with S'. □

"⇐": $A_1 \vee A_2 \vee A_3 \Rightarrow$ I is compliant with S'
With A_1 it follows that $\mathcal{H}_{red}$ still does not contain an entry related to n_{dest}. Therefore $\mathcal{H}_{red}$ could have been produced on S' as well; i.e., I is compliant with S'. The same applies to A_2 because the end entry of n_{src} had been written into $\mathcal{H}_{red}$ before the start entry of n_{dest} was logged.

After insertion of $n_{src} \rightarrow n_{dest}$, in any case, n_{src} has to be either executed or skipped before n_{dest} is activated or skipped. In addition, other (predecessor) nodes of n_{src}, which could have been executed parallel to n_{dest} so far may now have to be executed or skipped before n_{dest} can be marked. This node set is determined by $N_{critical}$ (see Fig. 7b). Only if each activity node of

$N_{critical}$ has either been marked as `SKIPPED` or has written its end entry before the start entry of n_{dest} into $\mathcal{H}_{red}$, the execution history can be produced on the new schema S' as well. This follows directly from A_3. □