Cumplimiento de Normativas en Procesos de Negocios

MSc. Ing. Laura González

Segundas Jornadas Uruguayas de
Gestión y Tecnologías de Procesos de Negocio

21 y 22 de Octubre de 2013

Instituto de Computación
Facultad de Ingeniería
Universidad de la República de Uruguay

Laboratorio de Integración de Sistemas

- Grupo académico-tecnológico del Instituto de Computación (INCO)
  - http://www.fing.edu.uy/inco/grupos/lins/

- Aborda la temática de **Integración de Sistemas**, en especial utilizando **Tecnologías de Middleware**.

Laboratorio de Integración de Sistemas

Principales Áreas de Trabajo

Plataformas de Desarrollo Empresarial
Java Enterprise Edition / .Net Framework

Sistemas de Información Geográfica
Bases de Datos Geográficas, Servidores de Mapas, Visualizadores

Middleware Convencional
Message Oriented Middleware (MOM), Integration Brokers, Servidores de Aplicaciones

Tecnología Móvil

Evaluación de Tecnologías

Middleware Avanzado
Web Services (SOAP Y REST), Enterprise Service Bus

Arquitecturas Orientadas a Servicios (SOA)

Middleware en Presentación
Portales Web, Mashups

Interoperabilidad y Estándares

Gobierno Electrónico (e-government)

Plataformas en Área Salud (e-health)

Inclusión Digital (e-inclusion)

Plataformas Científicas (e-science)

Agenda

- Introducción
  - Cumplimiento de Normativas / Conformidad de PNs
- Tipos de Requerimientos de Conformidad
- Modelado de Requerimientos de Conformidad
- Chequeo de Conformidad de PNs
- Soluciones para el Chequeo de Conformidad

Introducción

Motivación

- Las organizaciones deben actualmente cumplir con distintos tipos de normativas:
  - Políticas internas a una organización
    - Funcionales o no funcionales (QoS, seguridad, etc)
  - Acuerdos con otras organizaciones
    - Ej: Service Level Agreements (SLA)
  - Políticas externas a una organización
    - Políticas públicas (protección: datos personales, consumidor)
    - Normativas sectoriales (transporte, etc)
    - Normativas y estándares aplicables universalmente

(Turetken, Elgammal, van den Heuvel, & Papazoglou, 2011)

Introducción

Motivación

- Estas normativas hacen que las organizaciones tengan que:
  - Establecer sistemas de control interno
  - Evaluar continuamente sus Procesos de Negocio (PNs)
  - Asegurar que los PNs cumplan con las mismas

- Si no se garantiza la conformidad de los PNs con estas normativas, las organizaciones se enfrentan a riesgos de litigios y sanciones, incluso penales

(Turetken, Elgammal, van den Heuvel, & Papazoglou, 2011)

Introducción

Conformidad de Procesos de Negocio

- Business Process Compliance
  - Asegurar que los PNs cumplan con un conjunto de normativas acordadas

- Principales Problemáticas
  - Controles hechos “a mano”
  - Soluciones para problemas particulares comúnmente distribuidas en varios sistemas
    - dificulta verificar la conformidad de los PNs
    - falta de flexibilidad para adaptarse a cambios

(Turetken, Elgammal, van den Heuvel, & Papazoglou, 2011)

Introducción

Conformidad de Procesos de Negocio

- Surge entonces la necesidad de contar con soluciones integrales que permitan gestionar la conformidad de los PNs con estas normativas

- Algunas características deseables:
  - Gestionar los requerimientos de conformidad en todo el ciclo de vida de los PNs
  - Modelo conceptual que permita capturar los requerimientos de conformidad y su relación con los PNs
  - Gestionar estos requerimientos de forma separada a los PNs

(Turetken, Elgammal, van den Heuvel, & Papazoglou, 2011)

Agenda

- Introducción
- Tipos de Requerimientos de Conformidad
- Modelado de Requerimientos de Conformidad
- Chequeo de Conformidad de PNs
- Soluciones para el Chequeo de Conformidad

Tipos de Requerimientos de Conformidad

- En el marco del proyecto europeo COMPAS se identificaron categorías de requerimientos de conformidad:
  - Los tipos de Requerimientos Básicos hacen referencia a la estructura básica de un PN
  - Los tipos de Requerimientos Avanzados se construyen sobre los básicos

(Compas Project, 2008)

Tipos de Requerimientos de Conformidad

Tipos Básicos

- Flujo de Control
  - Abordan qué actividades se realizan y en qué orden
  - Ej: International Financial Reporting Standards (IFRS)
    - Aborda los procesos de reporte financiero de las organizaciones
- Locativo
  - Conciernen la ubicación en donde las actividades se desarrollan
  - Ej: Ley Sarbanes Oxley (SOX)
    - Hace referencia a la ubicación en donde se almacena la información

(Compas Project, 2008)

Tipos de Requerimientos de Conformidad

Tipos Básicos

- Información
  - Conciernen la información utilizada/producida en los PN
  - Ej: Basel II (leyes y regulaciones bancarias)
    - Requiere cierta información al dar una tarjeta de crédito para la posterior evaluación de riesgos
- Recursos
  - Abordan los recursos que se utilizan en los PNs (empleados, sistemas, etc)
  - Ej: Ley Sarbanes Oxley (SOX)
    - Separation of Duty

(Compas Project, 2008)

Tipos de Requerimientos de Conformidad

Tipos Básicos

- Temporal
  - Abordan cuándo se hacen las tareas (o cuándo no deben hacerse) en el contexto de un PN
    - Por ejemplo, en relación a otras tareas o eventos
  - Ej: Basel II (leyes y regulaciones bancarias)

(Compas Project, 2008)

Tipos de Requerimientos de Conformidad

Tipos Avanzados

- Monitoreo
- Pago
- Privacidad
- Calidad
- Seguridad
- Retención
- Transacción

(Compas Project, 2008)

Tipos de Requerimientos de Conformidad

Tipos Avanzados

- Calidad
  - Aborda el nivel de calidad en los PNs en relación:
    - al flujo de control (disponibilidad, confiabilidad, etc)
    - a la información (exactitud y completitud de la información)
  - Ej: HIPPA (Health Insurance Portability and Accountability Act)
    - Exactitud de la información personal de salud
- Retención
  - Archivado, recuperación y eliminación de la información
  - Involucra aspectos de información y temporales
  - Ej: MIFID (Markets in Financial Instruments Directive)
    - Documentos deben almacenarse al menos 5 años

(Compas Project, 2008)

Agenda

- Introducción
- Tipos de Requerimientos de Conformidad
- Modelado de Requerimientos de Conformidad
- Chequeo de Conformidad de PNs
- Soluciones para el Chequeo de Conformidad

Modelado de Requerimientos de Conformidad

- Un pre-requisito para verificar la conformidad de PNs es tener los requerimientos de conformidad en una forma procesable por máquina
- Existen distintos enfoques para el modelado, en particular:
  - Lineal Temporal Logic (LTL)
  - Compliance Rule Graphs (CRG)
- Nos vamos a enfocar en los requerimientos de Flujo de Control

(Reichert & Weber, 2012)

Modelado de Requerimientos de Conformidad

Lineal Temporal Logic (LTL)

- LTL agrega a la lógica proposicional tradicional un conjunto de operadores temporales que permiten "navegar" de un punto a otro en el tiempo
- Operadores
  - X: next
  - F: eventually
  - G: always
  - U:until
  - W:weakly until

(Reichert & Weber, 2012)

Modelado de Requerimientos de Conformidad

Lineal Temporal Logic (LTL)

- Ejemplos:
  - Antes de programar la cirugía, se debe informar al paciente de la anestesia
    - ¬Programar Cirugía **W** Informar de Anestesia
  - Luego de que un paciente es dado de alta, se debe escribir un informe de alta
    - **G** (Alta Paciente ⟹ **F** (Escribir Informe de Alta))

(Reichert & Weber, 2012)

Modelado de Requerimientos de Conformidad

Compliance Rule Graphs (CRGs)

- Dado que la especificación formal basada en LTL puede no resultar amigable para los expertos de dominio, se han desarrollado notaciones gráficas

- En particular, los Compliance Rule Graphs (CRGs) permiten modelar requerimientos de conformidad en base a:
  - Un patrón de precedencia
  - Un patrón de consecuencia

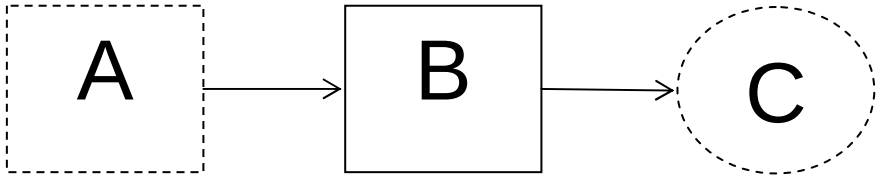
(Reichert & Weber, 2012)

Modelado de Requerimientos de Conformidad

Compliance Rule Graphs (CRGs)

- Ejemplos:

<E,D,F,G,B> - cumple
<C,**A**,**B**,G,D> - cumple
<A,D,B,G,**A**> - no cumple



<**A**,B,F,C,D> - cumple
<**B**,F,D,B,A> - cumple
<**B**,G,E,**C**,D> - no cumple

(Reichert & Weber, 2012)

Agenda

- Introducción
- Tipos de Requerimientos de Conformidad
- Modelado de Requerimientos de Conformidad
- Chequeo de Conformidad de PNs
- Soluciones para el Chequeo de Conformidad

Chequeo de Conformidad de PNs

- Una vez que los requerimientos de conformidad se modelaron, se puede chequear la conformidad de un PN contra ellos

- El chequeo se puede realizar en distintas etapas del ciclo de vida del PN, en particular:
  - Etapa de Diseño (a priori)
  - Etapa de Ejecución (runtime)
  - Luego de la Ejecución (a posteriori)

(Knuplesch, Reichert, Mangler, Rinderle-Ma, & Fdhila, 2013)

(Reichert & Weber, 2012)

Chequeo de Conformidad de PNs

Etapa de Diseño (a priori)

- El chequeo de conformidad a priori, verifica la conformidad de un PN antes que éste sea llevado al entorno de ejecución

- Un modelo de un PN cumple con un requerimiento de conformidad si sólo si el modelo sólo permite trazas que cumplen con ese requerimiento

- Se utilizan en general técnicas Model Checking

(Knuplesch, Reichert, Mangler, Rinderle-Ma, & Fdhila, 2013)

(Reichert & Weber, 2012)

Chequeo de Conformidad de PNs

Etapa de Ejecución (runtime)

- El chequeo a priori no siempre es posible:
  - Tamaño o complejidad de los PNs o requerimientos
  - Requerimientos dependientes de valores de ejecución
- Además los requerimientos de conformidad pueden variar en el tiempo

- En estos casos se puede monitorear el cumplimiento de la conformidad durante la ejecución de las instancias de un PN

(Knuplesch, Reichert, Mangler, Rinderle-Ma, & Fdhila, 2013)

(Reichert & Weber, 2012)

Chequeo de Conformidad de PNs

Etapa de Ejecución (runtime)

- Cuando se detecta, en tiempo de ejecución, que una instancia no cumple con un requerimiento existen situaciones en las cuales:
  - es posible reponerse al “no cumplimiento” (por ejemplo, ejecutando otra tarea)
  - no es posible reponerse al “no cumplimiento”

(Knuplesch, Reichert, Mangler, Rinderle-Ma, & Fdhila, 2013)

(Reichert & Weber, 2012)

Chequeo de Conformidad de PNs

Luego de la Ejecución (a posteriori)

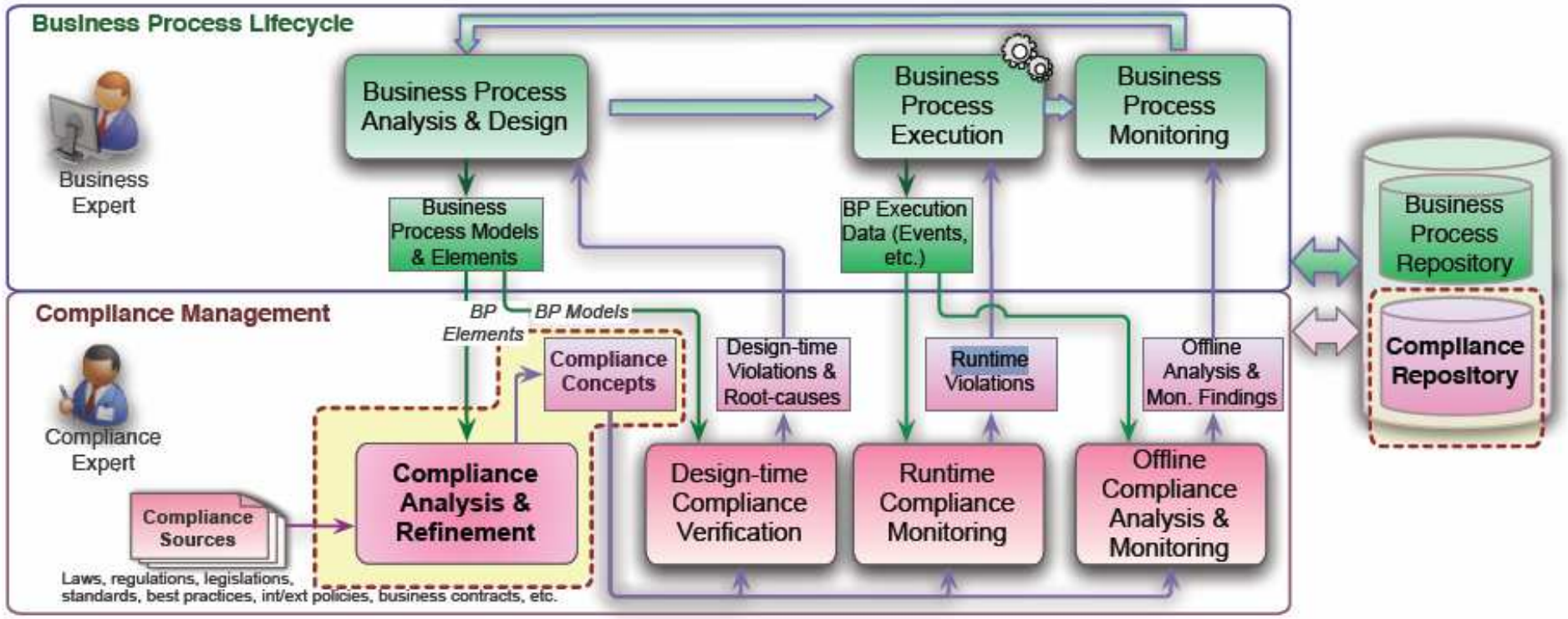
- Consiste en analizar los logs de ejecución de las instancias de un PN para determinar si cumplen con los requerimientos de conformidad

- Para este tipo de chequeo se puede utilizar también técnicas de Model Checking

(Knuplesch, Reichert, Mangler, Rinderle-Ma, & Fdhila, 2013)

(Reichert & Weber, 2012)

Chequeo de Conformidad de PNs



(Turetken, Elgammal, van den Heuvel, & Papazoglou, 2011)

Agenda

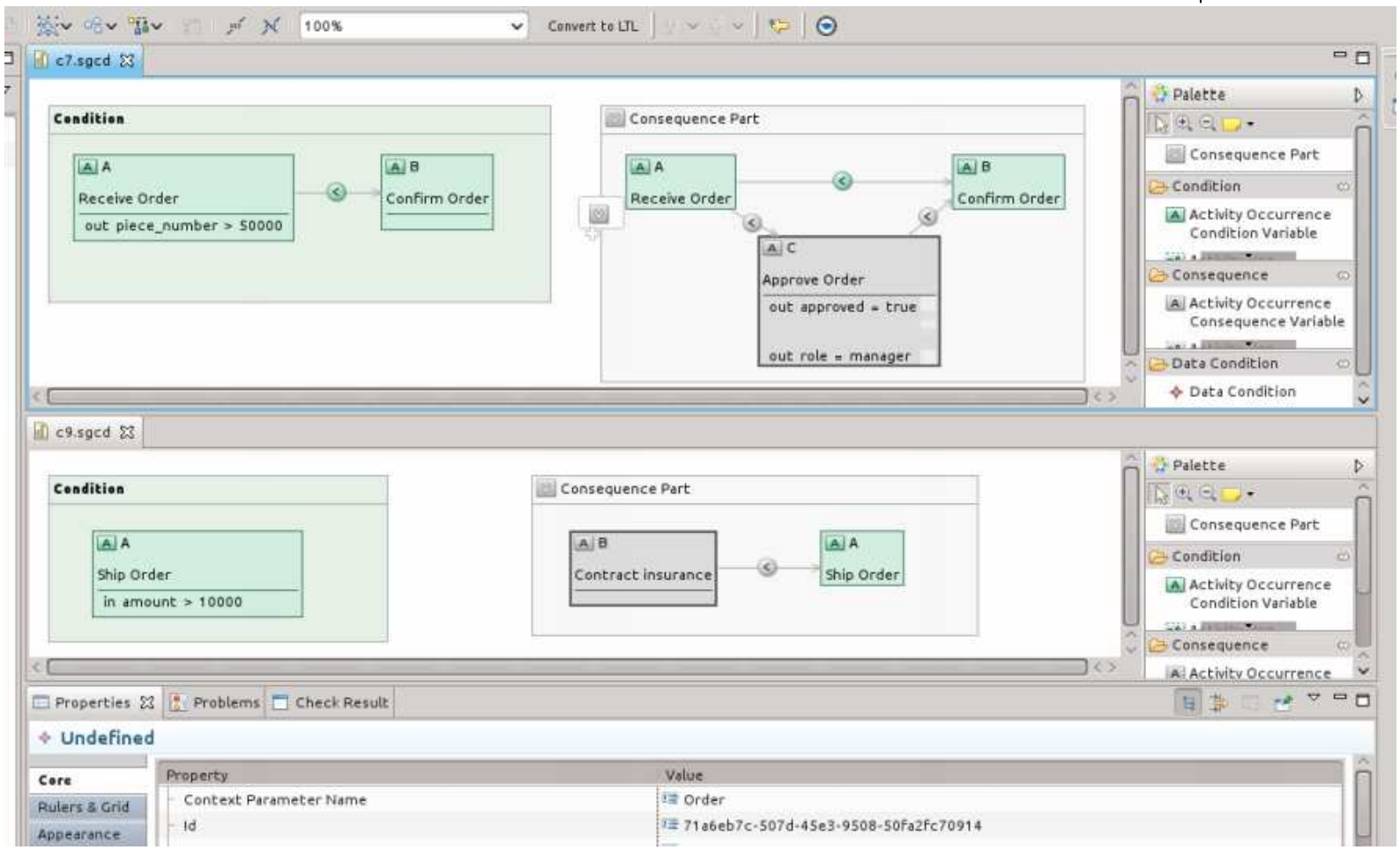
- Introducción
- Tipos de Requerimientos de Conformidad
- Modelado de Requerimientos de Conformidad
- Chequeo de Conformidad de PNs
- Soluciones para el Chequeo de Conformidad

Soluciones para el Chequeo de Conformidad de PNs

- SeaFlows
- Enterprise Service Bus
- Complex Event Processing

Soluciones para el Chequeo de Conformidad de PNs

SeaFlows

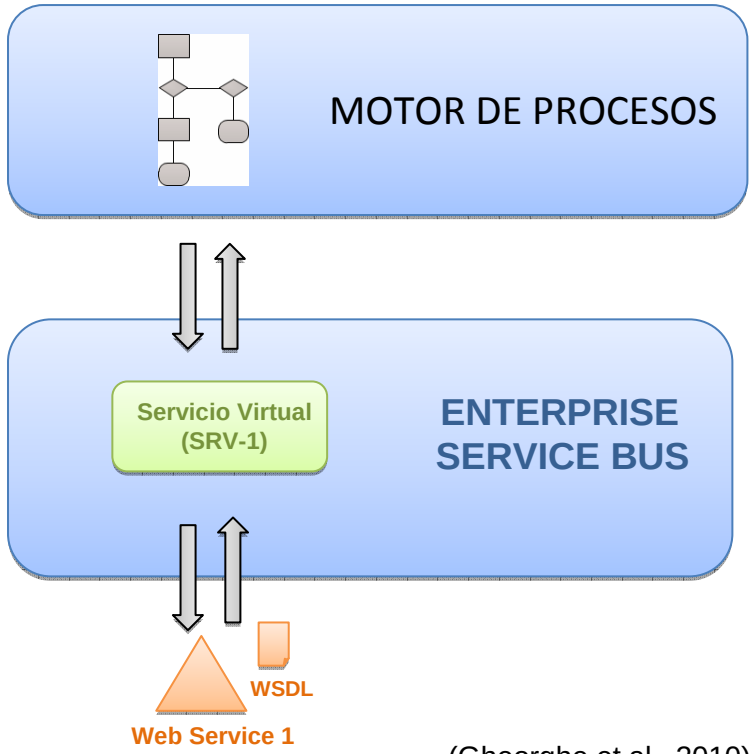


http://dbis.eprints.uni-ulm.de/939/2/Dissertation.pdf

Soluciones para el Chequeo de Conformidad de PNs

Enterprise Service Bus

- Plataforma de integración basada en estándares
- Principales capacidades:
  - conectividad
  - transformación de mensajes
  - ruteo inteligente
  - monitoreo
- Ejemplo de Aplicación
  - Ley de protección de datos personales

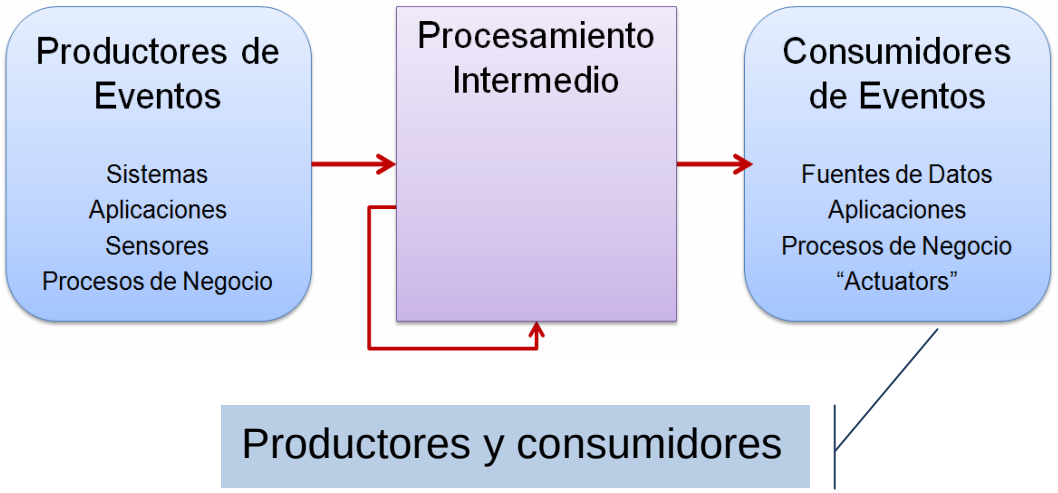


(Gheorghe et al., 2010)

Soluciones para el Chequeo de Conformidad de PNs

Complex Event Processing (CEP)

- Un evento se define en general como “algo que ocurre o es percibido como que ocurre”
- Un evento complejo es un evento que representa, o enmarca, un conjunto de eventos más simples



(Etzion & Niblett, 2010)

http://www.complexevents.com/wp-content/uploads/2011/08/EPTS_Event_Processing_Glossary_v2.pdf

Soluciones para el Chequeo de Conformidad de PNs

Complex Event Processing (CEP)

- Los motores CEP se podrían utilizar para monitorear el cumplimiento de normativas
- Sería deseable poder generar automáticamente la especificación de eventos complejos a partir de los requerimientos de conformidad
- Ejemplos:
  - Verificar que las interacciones entre organizaciones se ajusten a la coreografía acordada

(Baouab, Perrin, & Godart, 2011)

Resumen

- Se presentó la temática del cumplimento de normativas en PNs
- Se vieron distintos tipos de requerimientos de conformidad: básicos y avanzados
- Se presentaron formas de especificar requerimientos de conformidad: LTL y CRGs
- Se presentaron distintas etapas en las que se puede realizar el chequeo de la conformidad de PNs
- Se mostraron algunas soluciones para el chequeo

¡Muchas Gracias!

MSc. Ing. Laura González

lauragon@fing.edu.uy

Segundas Jornadas Uruguayas de

Gestión y Tecnologías de Procesos de Negocio

21 y 22 de Octubre de 2013

Instituto de Computación

Facultad de Ingeniería

Universidad de la República de Uruguay

Referencias

- Baouab, A., Perrin, O., & Godart, C. (2011). An Event-Driven Approach for Runtime Verification of Inter-organizational Choreographies. In 2011 IEEE International Conference on Services Computing (SCC) (pp. 640–647). Presented at the 2011 IEEE International Conference on Services Computing (SCC). doi:10.1109/SCC.2011.55
- Compas Project. (2008). State-of-the-art in the field of compliance languages.
- Gheorghe, G., Crispo, B., Schleicher, D., Anstett, T., Leymann, F., Mietzner, R., & Monakova, G. (2010). Combining Enforcement Strategies in Service Oriented Architectures. In P. Maglio, M. Weske, J. Yang, & M. Fantinato (Eds.), Service-Oriented Computing (Vol. 6470, pp. 288–302). Springer Berlin / Heidelberg.
- Knuplesch, D., Reichert, M., Mangler, J., Rinderle-Ma, S., & Fdhila, W. (2013). Towards compliance of cross-organizational processes and their changes. In Business Process Management Workshops (pp. 649–661).
- Reichert, M. U., & Weber, B. (2012). Enabling flexibility in process-aware information systems: challenges, methods, technologies. Springer.
- Turetken, O., Elgammal, A., van den Heuvel, W.-J., & Papazoglou, M. (2011). Enforcing Compliance on Business Processes through the use of Patterns. Retrieved from http://aisel.aisnet.org/ecis2011/5/