5
Casos de Leis

Apesar de existirem diversos trabalhos relevantes para assegurar a governabilidade de sistemas através de leis de interação, como identificados na seção 2.3, os trabalhos desenvolvidos até o momento, no contexto da especificação de requisitos para sistemas multiagentes abertos, não apresentam claramente o mapeamento e a documentação de requisitos de fidedignidade para infra-estruturas capazes de verificar em tempo de execução se os requisitos, ou melhor, se as regras são obedecidas.

Procura-se na abordagem aqui proposta, chamada Casos de Leis, prover uma maneira eficaz de registrar as decisões (o chamado rastro de *rationale*) para derivar requisitos de fidedignidade, que por sua vez, vão derivar as leis. Mais especificamente, a documentação iterativa de requisitos deve ser feita de forma a preservar o conjunto de decisões que foram tomadas e as razões que determinaram a escolha de requisitos ou de sua implementação.

Desta forma, Casos de Leis complementam os avanços obtidos na área de governança de sistemas multiagentes abertos com uma forma de documentação e modelagem baseada em um modelo conceitual adaptado da proposta original de Casos de Fidedignidade [41]. Acredita-se que a aplicação desta estrutura no contexto de sistemas multiagentes consiga representar, em diferentes níveis de detalhe, as decisões e os requisitos derivados a partir do entendimento do problema.

Requisitos de fidedignidade devem ser baseados em serviços que funcionem corretamente independentemente das ameaças que sofram. Neste contexto, existem quatro abordagens relevantes que lidam com requisitos de fidedignidade: casos de fidedignidade [41], casos de mau uso (*misuse cases*) [45], casos de uso de segurança (*security use cases*) [44] e análise de risco para derivar leis [43].

Um Caso de Fidedignidade [41] é uma documentação de evidências que provê um argumento válido e convincente quanto à fidedignidade de um artefato. O argumento baseia-se em uma estrutura que visa levantar evidências e provas de

que um dado sistema possui todos os atributos de fidedignidade necessários para uma determinada aplicação. Ou seja, é uma cadeia de raciocínio documentada, baseada em evidências. Quanto melhor for a argumentação e as evidências durante o raciocínio, maior a chance de a hipótese ser verdadeira e, conseqüentemente, mais convincente é o caso de fidedignidade. No processo de argumentação, é necessário pensar numa estratégia que provê a veracidade da hipótese. E, por sua vez, ao especificar uma estratégia talvez seja necessário especificar sub-hipóteses. Uma vez que todas as sub-hipóteses foram provadas, então se obtém a prova final da hipótese.

Considerando o processo acima, [41] propôs seis elementos que compõem um caso de fidedignidade: contexto, hipótese, estratégia, pressuposição, solução e evidência. A partir desta proposta, foi gerado um modelo conceitual de rastro do *rationale* adaptado.

Em conjunto com Casos de Fidediginidade, surgiram Casos de Mau Uso (*Misuse Case*) [45] e Casos de Uso de Segurança (*Security Use Cases*) [44] como técnicas de elicitação de requisitos eficientes para complementar os Casos de Leis. A abordagem de Casos de Mau Uso [45] é uma extensão da abordagem de Casos de Uso. O seu objetivo é modelar e especificar cenários negativos do sistema. Um Caso de Mau Uso é simplesmente um Caso de Uso do ponto de vista de um ator hostil ao sistema em construção e que não deveria poder ser realizado no sistema implementado. O ator pode ser tanto um ser humano, como um agente de software (inteligente ou não).

Casos de Mau Uso se adequam muito bem à análise de requisitos de ameaças de segurança causadas por intrusão (*security*) já que as ameaças do sistema correspondem às ações que um ser humano ou agente de software efetua de forma deliberada para afetar ou destruir o sistema. Novos Casos de Uso poderiam ser modelados com o objetivo de identificar essas ameaças e mapear em Casos de Mau Uso a fim de atenuá-las.

Além dos requisitos de segurança causados por intrusão, Casos de Mau Uso podem ser adaptados para quaisquer uns dos atributos de fidedignidade, tais como confiabilidade, disponibilidade ou segurança contra acidentes (*safety*). Estes atributos podem ser elicitados e analisados como ameaças causadas por agentes que não são necessariamente inteligentes. Tais agentes poderiam ser: erros humanos, tempestades, erros de projeto (*bugs*), problemas na rede, entre outros.

Eles podem causar diversos tipos de falhas no software. Como Casos de Mau Uso enfatizam ameaças e não requisitos de segurança propriamente ditos, Casos de Uso de Segurança (*Security Use Cases*) surgiram como uma forma de estender Casos de Mau Uso com o objetivo de suprir esta deficiência.

Casos de Uso de Segurança [44] têm por objetivo analisar e especificar requisitos de segurança contra as quais a aplicação deve se proteger considerando um elenco de ameaças previamente identificado. Basicamente, a descrição de um Caso de Uso de Segurança contém a identificação do Caso de Uso e do caminho que o levou a ser ativado, da ameaça de segurança, das pré-condições, das interações dos usuários, dos usuários de mau uso, do sistema, das ações do sistema e das pós-condições. Sendo que, as interações do sistema, ações do sistema, e as pós-condições devem ser especificadas como requisitos do sistema, e os outros não.

Além das abordagens apresentadas baseadas em Casos de Uso, métodos de análise de risco podem ser estruturados para auxiliar na especificação, desenvolvimento, monitoração e manutenção dos requisitos de sistema e com o objetivo de aumentar a fidedignidade. Como visto em [43], requisitos de fidedignidade podem ser modelados como riscos, que por sua vez, guiam na especificação das leis. Em [43], é proposto um formulário de cenários para especificar riscos, manter o rastro de causas e conseqüências, descrever quais atributos de fidedignidade as conseqüências são afetados, e especificar a decisão da solução.

Dadas as abordagens apresentadas, através da aplicação de Casos de Mau Uso em diferentes contextos, e da abordagem dos Casos de Uso de Segurança, foi possível mapear com uma certa facilidade, o uso das duas abordagens e da proposta de Casos de Uso como primeira etapa de um processo de derivação de leis de interação de agentes. Entretanto, notou-se a falta do *rationale* a respeito das interações dos usuários e sistemas, que levassem a garantia de que o caso de uso de segurança fosse adequado para lidar com o problema identificado. Este problema foi resolvido através da adaptação de Casos de Fidedignidade, já que estes são uma forma de estruturar a documentação de argumentos e evidências de que o sistema atende a requisitos de fidedignidade.

Desta forma, Casos de leis conjugam a aplicação de casos de uso e casos de fidedignidade. A abordagem de casos de uso é útil para mantermos uma visão

geral sobre os requisitos que são identificados e casos de fidedignidade são úteis para registrar o detalhamento da análise.

Em nossos experimentos, o uso de análise de risco, ou uma postura em identificar claramente potenciais problemas que serão abordados futuramente, tem se mostrado bastante promissor no intuito de promover a identificação e o detalhamento de estratégias para mitigar potenciais problemas. Além disto no contexto de criticalidade, esta abordagem pode ser utilizada para determinar valores referentes ao nível de variação no monitoramento da importância de agentes.

Nas próximas subseções são apresentados: a descrição do exemplo utilizado ao longo do capítulo com o objetivo de ilustrar os conceitos apresentados, a abordagem de Caso de Leis com seu modelo conceitual, e o processo de utilização com um exemplo de aplicação para a abordagem proposta. O capítulo termina com o desenvolvimento de casos de leis à partir do exemplo detalhado na próxima seção.

5.1. Descrição do Exemplo

Esta seção irá apresentar o exemplo escolhido para ilustrar o desenvolvimento de Casos de Leis, chamado *Supply Chain Management* (SCM). O SCM é o planejamento e coordenação das atividades de uma cadeia de suprimentos [48]. Essas atividades podem ter vários participantes e organizações, e a coordenação desses participantes é um ponto chave para uma cadeia eficiente. O *Supply Chain* não está relacionado apenas com os produtores e fornecedores, mas também com transportadoras, centros de distribuição, e clientes. Essa cadeia é extremamente dinâmica e envolve um grande fluxo de informação, produtos e recursos financeiros entre diferentes estágios.

O TAC SCM [46] é um jogo que foi desenvolvido por pesquisadores do laboratório de *e-Supply Chain Management* da *Carnegie Mellon University* e *Swedish Institute of Computer Science* (SICS). Ele foi modelado para capturar a complexidade de uma cadeia de suprimentos dinâmica, porém com regras simples para que muitas equipes possam participar dessa competição. Basicamente, seis agentes "produtores de PC" participam em cada jogo do TAC SCM. Esses

participantes competem por clientes com incerteza na demanda e por peças de um número limitado de fornecedores. Todo dia, os clientes enviam pedidos de cotações e selecionam as melhores ofertas baseadas no preço e na data de entrega. Os agentes são limitados pela capacidade da fábrica, e tem que gerenciar a compra de peças de oito fornecedores. Quatro componentes são precisos para montar um PC: CPU, Placa Mãe, Memória, e Disco Rígido. Cada componente está disponível em diferentes modelos. O jogo começa quando um ou mais agentes se conectam ao servidor do TAC SCM. O servidor simula o comportamento dos fornecedores e clientes, e oferece um ambiente para cada participante com um banco para sua conta corrente, uma fábrica, e estoques de peças e PCs. No final do jogo, o agente que possuir o maior valor de dinheiro na conta corrente é declarado o vencedor.

O jogo apresenta um bom nível de complexidade, pois cada agente deve competir em vários mercados por diferentes componentes do lado dos fornecedores, e em mais outros mercados por diferentes tipos de PCs no lado dos clientes. Além disso, todos esses mercados possuem interdependências e incertezas. A figura abaixo ilustra o cenário.

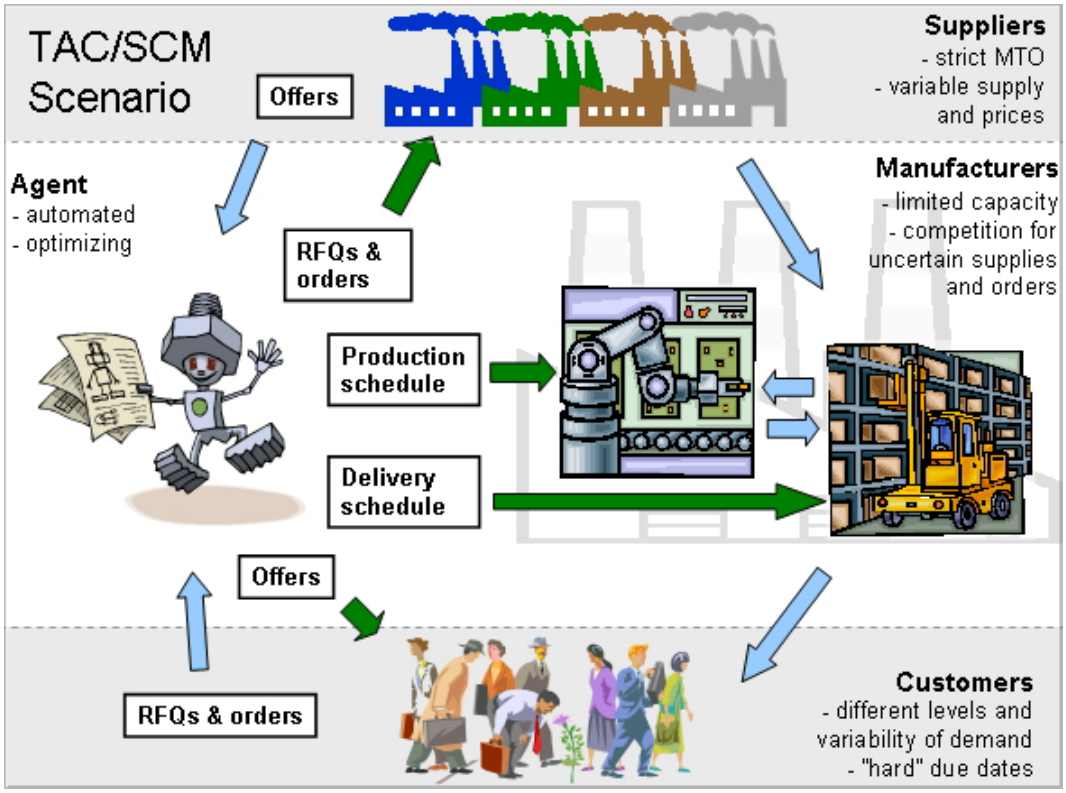

Figura 26 - Cenário do jogo TAC SCM

5.2.
Caso de Leis

Um Caso de Leis é um documento de evidências que provê um argumento válido e convincente que mostra que um SMA aberto exibe todos os seus atributos de fidedignidade requeridos *a priori* para uma dada aplicação num dado ambiente através do *rationale* da derivação de elementos de leis.

Casos de leis associam a aplicação de casos de uso e casos de fidedignidade. O primeiro é útil para mantermos uma visão geral sobre os requisitos que são identificados e o segundo é útil na documentação das decisões que são tomadas e o *rationale* em torno desta decisão. A decisão está diretamente relacionada à criação de leis de interação que serão verificadas e aplicadas em tempo de execução.

Para desenvolver Casos de Leis, é necessário desenvolver os Casos de Uso e gerar o documento de requisitos funcionais do sistema. Feito isso, faz-se necessário levantar as ameaças do sistema através dos requisitos e refinar os Casos de Leis iterativamente, baseando-se sempre nos requisitos funcionais e não funcionais. Após ter gerado os Casos de Leis, deve ser feito uma análise dos mesmos para gerar os requisitos de leis que, por sua vez, podem ser mapeados para a linguagem de especificação XMLaw.

Em um sistema real, com várias necessidades e propriedades que precisam ser satisfeitas, é natural que a quantidade de informações derivadas de um processo de análise cresça com o desenvolvimento da aplicação, isto implicará em um número considerável de hipóteses e argumentos. Para facilitar o entendimento da documentação por parte de um leitor, é proposta, em conjunto com a proposta original de casos de fidedignidade, uma notação gráfica para a representação de elementos (Figura 27).

Pequenas adaptações para a notação proposta foram definidas, em prol de adequá-la ao português e também com o objetivo futuro do uso de uma ferramenta de modelagem própria para a elaboração desta proposta.

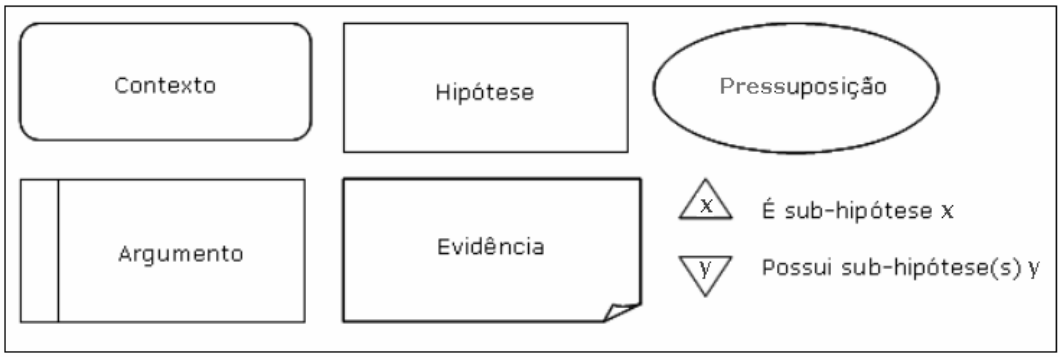

Figura 27 - Notação Gráfica

O ponto principal da proposta de casos de fidedignidade está na estrutura dos argumentos e das evidências que apóiam e corroboram este argumento. Casos de fidedignidade formais ou informais devem ter como principal objetivo convencer um leitor da sua validade perante as necessidades identificadas. Desta forma, este documento é um elemento chave em nossa abordagem de governança de leis, sendo responsável por registrar todas as hipóteses, pressuposições, contextos e argumentos adotados no processo de derivação de leis de interação. Todos estes elementos estão estruturados em um modelo conceitual.

O modelo conceitual apresentado na Figura 28 é derivado da aplicação da proposta original de casos de fidedignidade a problemas de governança de leis.

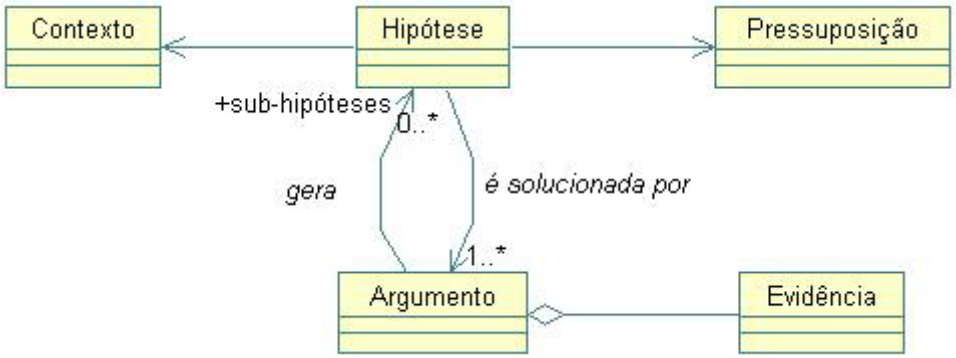

Figura 28 - Modelo Conceitual

Analisando a Figura 28, o ponto principal de destaque é a possibilidade de descrever o conhecimento parcial sobre o sistema em desenvolvimento. Isto é, uma hipótese baseia-se em pressuposições e contextos e é solucionada por um conjunto de argumentos que são justificados por evidências. Pressuposições não precisam ser provadas, são assumidas como verdade e servem para caracterizarmos melhor o cenário abordado. O contexto nada mais é do que informações que especializam o problema e definem melhor o escopo de análise. Por sua vez, um argumento pode identificar novos contextos que derivam novas

hipóteses que necessitam de mais argumentos para o completo entendimento da solução. Por outro lado, a partir de um argumento é possível comprovar a hipótese através de evidências por meio de informações e dados coletados experimentalmente ou ainda por terem passado por um processo de verificação de corretude.

Casos de fidedignidade são derivados a partir de hipóteses sobre um sistema e da demonstração de que evidências que comprovem que as hipóteses são verdadeiras. A Figura 29 descreve o processo de desenvolvimento do *rationale* de um Caso de Leis utilizando o modelo conceitual adaptado. Esta estrutura permite uma maior compreensão e um melhor detalhamento da solução em proposta.

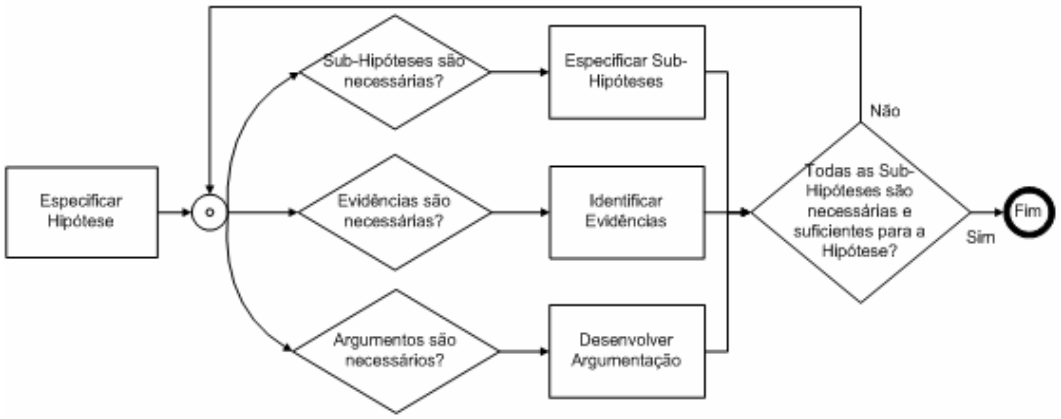

Figura 29 - Desenvolvendo o *rationale* de um Caso de Leis

Com o objetivo de exemplificar o *rationale* de um caso de leis, ilustramos na Figura 30 a especificação da sub-hipótese "o agente fornecedor de peça não pode falhar". Neste Caso de Leis, basicamente, deseja-se impedir que um fornecedor deixe de efetuar uma entrega.

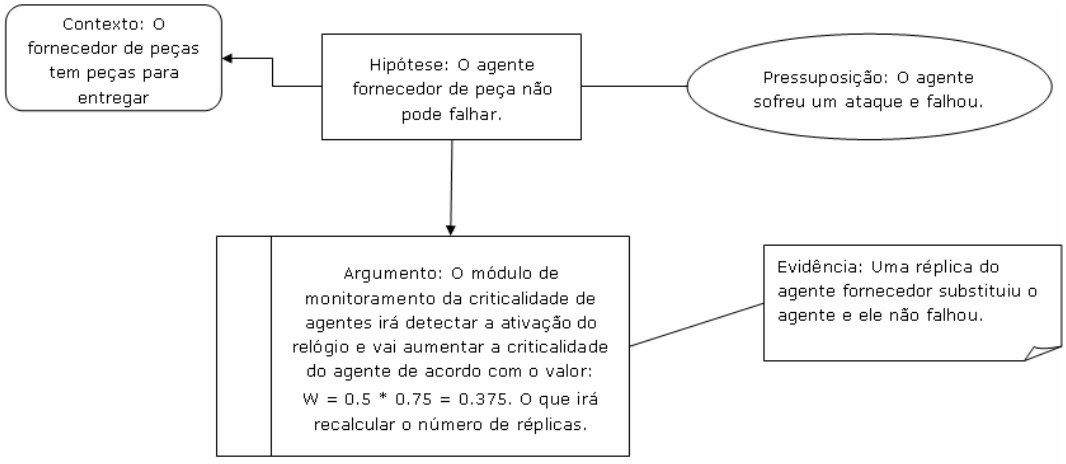

Figura 30 - Exemplo da Especificação de uma Sub-Hipótese

5.3.
Desenvolvendo Casos de Leis

Como mencionado anteriormente, para desenvolver Casos de Leis, é necessário que o Analista de Sistemas desenvolva os Casos de Uso e gere o documento de requisitos funcionais do sistema que, por sua vez, vão gerar os bens e serviços disponíveis pelo sistema. Feito isso, a partir dos requisitos não funcionais, o desenvolvedor vai levantar as ameaças para Caso de Uso, quando houver, e vai desenvolver os Casos de Leis iterativamente, baseando-se sempre nos requisitos funcionais, não funcionais e ameaças do sistema.

Após ter gerado os Casos de Leis, deve ser feito uma análise dos mesmos para gerar os requisitos de leis que, por sua vez, podem ser facilmente mapeados para a linguagem de especificação XMLaw. Na Figura 31, vemos de forma abstrata o processo de análise e projeto de leis utilizando casos de leis e as responsabilidades envolvidas.

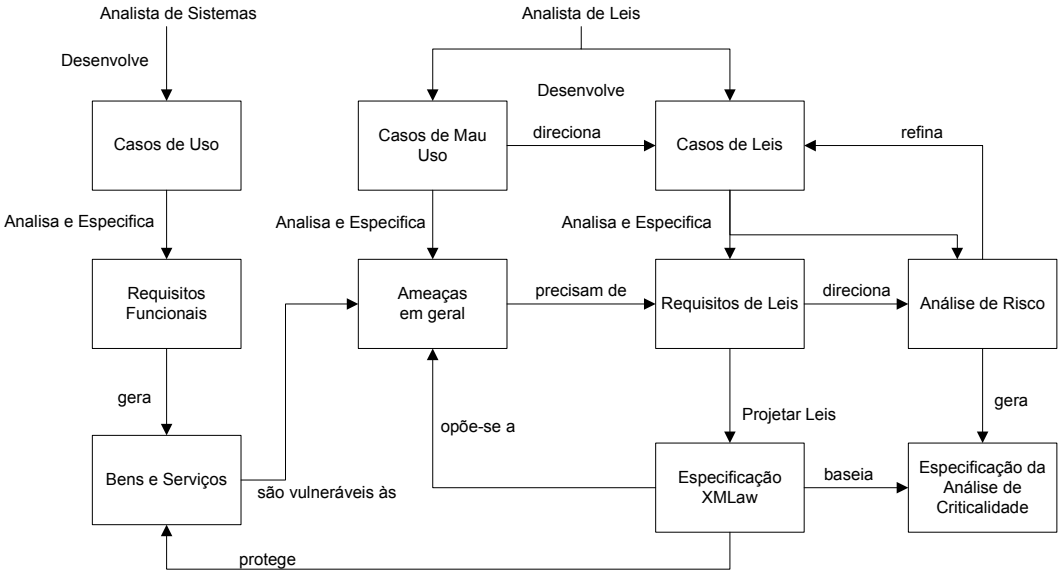

Figura 31 - Processo de Análise e Projeto de Leis

Utilizando um processo de análise e projeto de leis de forma iterativa, é possível refinar não somente as ameaças do sistema, como os requisitos de leis que atenuam tais ameaças.

5.4.
Diagrama de Casos de Leis

O diagrama de casos de leis estende o diagrama de casos de uso e é uma adaptação do diagrama de casos de uso de segurança [44]. Ele é composto por atores, casos de uso, casos de leis e riscos.

Os atores são os usuários do sistema, sejam eles seres humanos, agentes de software ou outros sistemas. Os casos de leis, fazendo uma analogia com os casos de uso de segurança, no diagrama, vão atenuar os riscos do sistema para fazer com que os requisitos de fidedignidade sejam atendidos e os casos de uso implementados com sucesso. A figura abaixo exibe a notação gráfica dos elementos de um diagrama de casos de leis:

Figura 32 - Notação Gráfica: Diagrama de Casos de Leis

Na Figura 33 (página seguinte) é ilustrada uma parte do Diagrama de Casos de Leis para o TAC SCM. Note que, para cada risco (elipse mais escura), existe pelo menos um caso de leis (elipse com um L dentro) que deriva leis de regulação para que a ameaça não tenha sucesso.

5.5.
Caso de Leis e Análise de Criticalidade

Com o objetivo de especificar os dados necessários para o monitoramento da criticalidade do agente, um Caso de Leis identifica o risco que está associado àquele determinado caso, analisa a probabilidade e impacto caso o risco efetivamente ocorra, e identifica o evento da interação entre os agentes que detecte a ocorrência do risco. Um evento da interação detalha o contexto da ocorrência e detalha como o risco pode ser detectado. Ele é importante no caso da especificação de leis porque vai determinar qual o evento da interação no qual aquele risco está inserido e que vai determinar a variação da criticalidade do agente.

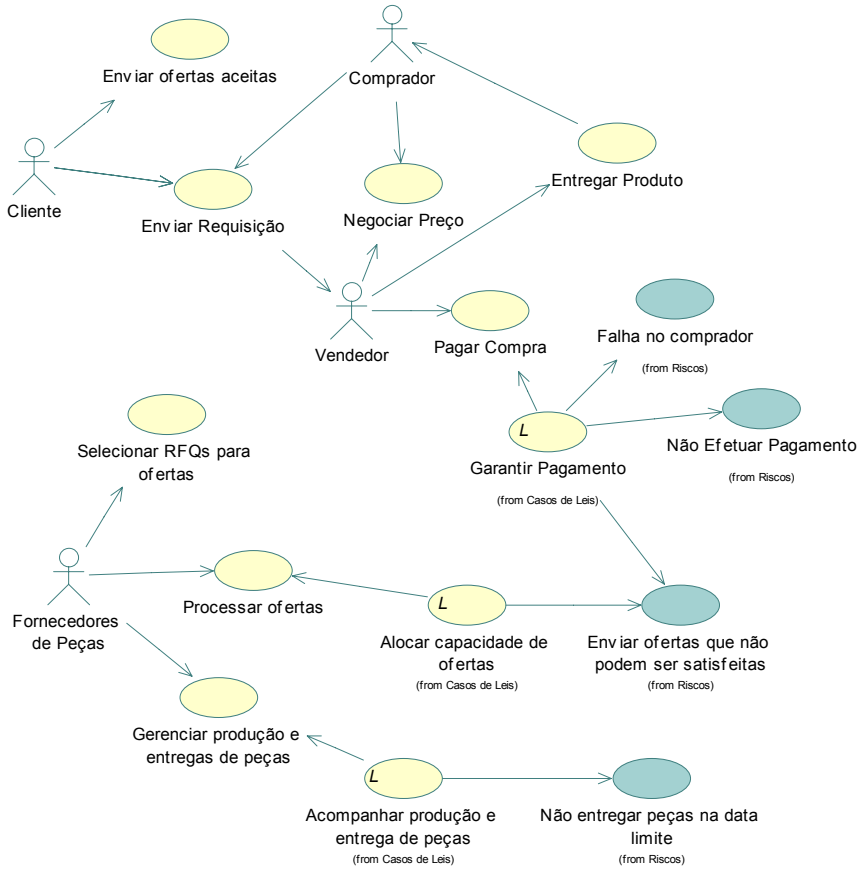

Figura 33 - Diagrama de Casos de Leis

Como visto, métodos de análise de risco podem ser estruturados para auxiliarem na engenharia dos requisitos do sistema e aumentarem a fidedignidade do mesmo. Em [43], requisitos de fidedignidade são modelados como riscos, que por sua vez, guiam a especificação das leis. Baseando-se nisso, o uso de análise de risco para apoiar a derivação de leis e mensurações de criticalidade de agentes está inserido na abordagem proposta.

Um Caso de Leis identifica o risco que está associado àquele determinado caso, analisa a probabilidade e impacto caso o risco efetivamente ocorra e identifica o evento da interação que detecte a ocorrência do risco.

A probabilidade é estimada seguindo a classificação definida pelo Departamento de Defesa dos Estados Unidos [47] e é uma classificação do risco com sua respectiva associação de um valor. Um risco pode ser classificado como improvável de ocorrer (0 a 20%), remoto (20% a 40%), ocasional (40% a 60%), provável (60% a 80%) ou freqüente (80% a 100%). A análise da classificação foge ao escopo deste trabalho.

O impacto do risco é estimado também seguindo a classificação definida em [47] e são: catastrófico]0,75;1], crítico]0,5;0,75], marginal]0,25;0,5] ou negligenciável]0;0,25]. Um risco catastrófico é capaz de causar morte, grandes perdas financeiras ou perda total do sistema. Um risco crítico é capaz de causar um ferimento grave, invalidez, alguma perda financeira ou grande perda do sistema. Um risco marginal é capaz de causar um ferimento leve ou pouca perda do sistema. E um risco negligenciável é incapaz de causar qualquer uma das perdas mencionadas.

Um evento da interação detalha o contexto da ocorrência e detalha como o risco pode ser detectado pelo sistema. Ele é importante no caso da especificação de leis porque vai determinar qual o evento da interação do protocolo no qual aquele risco está inserido e que vai determinar a variação da criticalidade do agente.

Identificado o evento da interação do protocolo durante a especificação da criticalidade no XMLaw, faz-se necessário detectar o peso, ou melhor, a importância do evento quanto à variação da criticalidade. O peso W será igual a P x I, onde P é a probabilidade do risco e I o impacto do risco associado àquele evento.

Referenciando a Figura 31, vemos que a análise de risco deve se dar após uma versão preliminar dos Casos de Leis a fim de refiná-los e gerar novos requisitos de leis, caso necessário. Uma vez finalizados a análise de risco, os refinamentos e os requisitos de leis e, por último, o projeto da especificação das leis em XMLaw, a especificação da variação da criticalidade dos agentes é feita, tendo como base a própria especificação XMLaw e os Casos de Leis previamente refinados com a análise de risco.

Já na Figura 34, é ilustrado o detalhamento de um caso de leis, "Acompanhar produção e entrega de peças" que está associado ao caso de uso "Gerenciar produção e entregas de peças" e que tem como objetivo impedir que o risco "Não entregar peças na data limite" ocorra. Note que a partir do *rationale* é possível identificar os elementos que serão especificados no XMLaw, como *Clock* (relógio) e *Norm* (norma). Neste exemplo, podemos ver um exemplo com a hipótese principal gerando as sub-hipóteses, que serão geradas e documentadas a parte, e a especificação do risco, probabilidade e impacto.

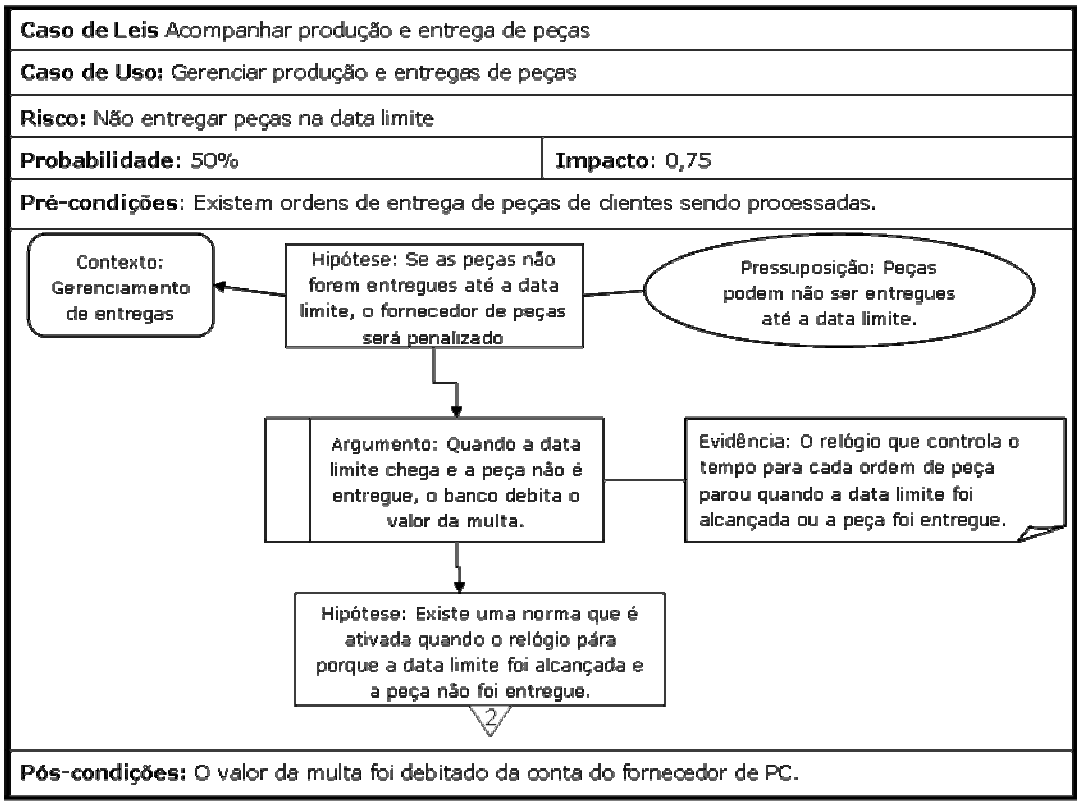

Figura 34 - Casos de Leis: Detalhamento

Considerando o risco de falha do fornecedor de peças presente no caso de leis ilustrado na Figura 30, para se estimar o peso da criticalidade associado a este evento, bastaria multiplicar a probabilidade pelo impacto do risco se concretizar, isto é 50%*0,75 = 0,375. E, no componente de criticalidade do XMLaw, existiria o seguinte código:

```
…
<Increase event-id="obligation_of_payment" event_type="norm_activation" value="0375" >
        <Assignee role-ref="customer" role-instance="$manufacturer.instance" />
</Increase>
…
```

Tabela 4 - Exemplo de Especificação de Aumento de Criticalidade