Makalah Seminar SeNTIK 2017 – STMIK JAKARTA STI&K
26 Juli 2017

IDENTIFIKASI *PROCESS-BASEDFRAUD* DALAM APLIKASI TABUNGAN MENGGUNAKAN LEVEL *EVENT LOGS*

Solichul Huda
Universitas Dian Nuswantoro
Jl. Imam Bonjol 107 Semarang
Solichul.huda@dsn.dinus.ac.id

ABSTRAK

Fraud dalam aplikasi tabungan sebagian disebabkan oleh proses yang melanggar Standard Operating Procedure (SOP); fraud tersebut dikenal dengan istilah Process-based Fraud (PBF). Beberapa metode deteksi fraud sebelumnya tidak bisa mendeteksi fraud dalam aplikasi tabungan, paper ini mengusulkan level event logs untuk mengidentifikasi informasi tindakan pertugas (originator) yang menjalankan proses. Pertama, mengidentifikasi rangkaian tindakan/perilaku originator, dan merancang level event logs. Selanjutnya, berdasarkan perilaku originator, dihitung attribute value, bobot penting atribut dan bobot fraud. Hasil uji coba dari data testing menunjukkan bahwa metode level event logs ini dapat mengidentifikasi pelanggaran SOP dalam aplikasi tabungan yang memiliki SMS banking dengan akurasi yang lebih baik 0.01 dibanding metode sebelumnya..
***Kata Kunci**: Process-based Fraud, originator, attribute value, bobot penting atribut, sms Banking.*

PENDAHULUAN

Fraud menjadi tema menarik penelitian semenjak fraud menjadi penyebab kerugian perusahaan [1]. Fraud menyebabkan kerugian mencapai angka 5 % [2]. Jumlah kerugian tersebut akan meningkat meningkat setiap tahunnya. Kerugian ini berpengaruh terhadap perusahaan besar maupun kecil.

Dari beberapa kejadian fraud menunjukkan pola yang berbeda dari setiap kejadian. Fraud juga terjadi di semua bagian dalam perusahaan. Dalam perbankan fraud dapat terjadi pada bagian keuangan maupun operasional, misalnya dalam aplikasi kredit dan aplikasi tabungan. Fraud dalam aplikasi kredit sebagian besar berupa kredit fiktif. Sedangkan dalam aplikasi tabungan sebagian berupa pelanggaran SOP dalam validasi SMS banking. Karena modeus pembobolan bank sebagian dilakukan lewat SMS banking, maka paper ini melaporkan penelitian tentang fraud dalam aplikasi tabungan yang memiliki fasilitas SMS banking.

Perusahaan perbankan perlu mengembangkan deteksi fraud dalam tabungan, semenjak marak terjadi fraud dalam aplikasi tersebut. Perbankan sendiri sebetulnya sudah memiliki anti fraud, namun sistem keamanan yang mereka miliki tidak dapat mendeteksi pelanggaran prosedur yang dilakukan oleh staf. Antifraud tersebut perlu dikembangkan sehingga antrifraud tersebut dapat mengidentifikasi pelanggaran SOP yang terjadi dalam bentuk SMS banking. Untuk mengidentifikasi fraud dalam transaksi

menggunakan pendekatan data mining, sedangkan untuk mengidentifikasi pelanggaran SOP menggunakan pendekatan process mining [3].

Ddeteksi fraud menggunakan process mining diantaranya menggunakan analisis performnace [4], algoritma ARL [5], algoritma ARL dan process mining hybrid [6], fuzzy MADM [7].

Dalam [7], indikator PBF menentukan akurasi deteksi PBF dalam aplikasi kredit. Namun indikator tersebut tidak dapat digunakan untuk mengidentifikasi fraud dalam aplikasi tabungan yang memiliki fasilitas sms banking. Dalam analisis awal menunjukkan bahwa Indikator tersebut tidak mampu menganalisis proses secara rinci. Paper ini mengusulkan level event logs level yang mampu menganalisis proses lebih rinci. Level event logs ini akan menggunakan level dibawahnya untuk mengontrol pelaksanaan sebuah proses/event. Hipotesis kami, level event logs dapat mengidentifikasi pelanggaran SOP dalam dalam proses yang rinci.

Dalam penelitian [3,4,5] fraud diidentifikasi menggunakan metode-metode process mining, diantaranya performance analisis, event sequence analisis, control flow dan analisis role. Implementasi metode tersebut menggunakan aplikasi ProM. Hasil analisis tersebut menjadi dasar penentuan menentukan suspicious fraud atau bukan.

Dalam [4], peneliti menggunakan process mining untuk mitigasi fraud. Mereka menggunakan analisis role, analisis event sequence, analisis performance untuk menganalisis proses bisnis. Namun, penelitian tersebut tidak menggunakan algoritma untuk mendeteksi fraud. Hasil penelitian tersebut membuktikan bahwa process mining dapat digunakan untuk mendeteksi fraud.

Konsep 1 + 5 + 1 diusulkan untuk mendeteksi fraud [4]. Konsep 1 + 5 + 1 terdiri dari 1. Persiapan log, 1. Analisis log 2. Analisis proses 3. Analisis conformance 4. Analisis sosial 5. Analisis performance 1. Iterasi dan refocus. Penelitian ini tidak menjelaskan bentuk dari fraud, dan penentuan fraud dilakukan secara subjektif oleh pakar. Penelitian ini menyimpulkan bahwa process mining dapat digunakan untuk mendeteksi fraud dalam berbagai process bisnis.

Process mining untuk mendeteksi fraud juga dilakukan menggunakan fuzzy MADM [7]. Mereka menggunakan analisis role, analisis proses, analisis throughput time, analisis skip, analisis wrong duty dan analsis event parallel untuk menganalisis proses binis. Fuzzy digunakan untuk menentukan bobot pelanggaran pada masing-masing indikator, dimana dengan MADM indikator tersebut dapat ditentukan sebagai fraud atau bukan. Penelitian tersebut dapat menentukan sebuah pelanggaran SOP dalam bentuk pelanggaran ringan. Namun perilaku pengguna yang menjalankan proses belum dipertimbangkan dalam menentukan bobot pelanggaran.

METODE PENELITIAN

Data event logs ini diambil dari aplikasi tabungan bank pemerintah yang diambil pada periode Juni 2014 – Mei 2016. Event logs ini berisi informasi tentang kode event, nama event, nama originator, tanggal dan jam mulai menjalankan event dan tanggal waktu selesai event.

Event logs ini dibagi menjadi dua, yaitu data training dan data testing, dimana dalam penelitian ini data training berjumlah 5.926 case, sedangkan data testing berjumlah 4.125.

Penelitian ini dilakukan dengan tahapan sebagai berikut :

1. Merancang level event logs
2. Analisis proses bisnis, penentuan attribute value, penentuan bobot

penting atribut dan penentuan bobot fraud

Process mining

Process mining merupakan pendekatan baru untuk menggali informasi dari event logs. Sebuah event logs terdiri dari satu set event. Setiap event terdiri dari kode case, kode event, nama event, nama originator, waktu mulainya event dan waktu berakhirnya event. Contoh event dalam aplikasi tabungan diantarnya pembukaan rekening, penarikan tunai, setoran tunai, dan penarikan SMS banking. Satu set event yang sejenis dikenal dengan istilah process instans atau case.

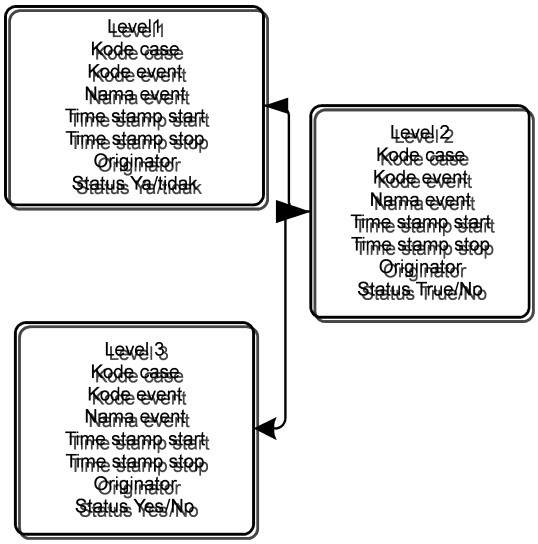
Ada tiga tipe process mining yaitu discovery, conformance dan enhancement. Dalam penelitian ini, process mining yang digunakan adalah conformance yaitu membandingkan case dengan SOP aplikasi tabungan. Sebuah pelanggaran case terhadap SOP disebut dengan atribut / indikator fraud.

MERANCANG LEVEL EVENT LOGS

Dalam penelitian [6] event logs yang digunakan adalah event logs 1 level. Untuk mendeteksi fraud pada aplikasi tabungan, butuh informasi tentang proses manual yang dilakukan oleh staf Back Office (BO) / originator. Penelitian ini mengusulkan level event logs dengan cara memasukkan proses manual dan hasilnya pada level dibawahnya. Level satu digunakan untuk event logs transaksi, kemudian level 2 dan seterusnya untuk event logs rinci dari proses yang dijalankan oleh staf BO tersebut. Berikut ini level event logs mulai level 1 sampai level 3.

Kode case
Kode event
Nama event
Awal mulainya event
Akhir jalannya event
Originator
Status event “Ya/Tidak”
Level 2
Kode case
Kode event
Awal mulainya event
Akhir jalannya event
Status event “True/No”
Level 3
Kode case
Kode event
Awal mulainya event
Akhir jalannya event
Status event “Yes/No”

Gambar 1 menjelaskan hubungan atau relasi antar event logs.



Gambar 1. Relasi antar event logs

Dari level event logs tersebut dapat diperoleh informasi tentang pengecekan KTP nasabah oleh originator atau staf BO. Event logs level 3 untuk menyimpan proses pengambilan data digital KTP dan foto nasabah. Level 2 untuk menyimpan proses pencocokan antara foto digital KTP dengan foto nasabah. Level 1 untuk menyimpan proses validasi identitas nasabah. Dari event di event logs level 1 tersebut dapat

diketahui bahwa BO sudah memvalidasi KTP nasabah.

ANALISIS PROSES BISNIS

Analisis proses bisnis menunjukkan ada atau tidaknya penyimpangan case terhadap SOP. Penyimpangan yang terjadi dikenal dengan istilah atribut/indikator fraud. Tabel 1 menunjukkan atribut / indikator fraud dalam sebuah proses bisnis.

Untuk mengidentifikasi pelanggaran SOP, penelitian ini menggunakan metode dalam process mining untuk menganalisis proses bisnis. Metode-metode tersebut diantaranya analisis skip, analisis throughput time, analisis duty, analisis resource, analisis decision dan analisis event parallel.

A. Analisis *skip*

Metode ini berfungsi untuk menganalisis sebuah proses yang meloncat satu atau lebih *event* merujuk pada urutan *control flow*. Jika lompatan terjadi pada *event sequence*, maka itu akan menambah nilai atribut *skip sequnce.* Namun jika lompatan terjadi pada *event decision*, itu akan berpengaruh pada atribut *skip decision*.

B. Analisis *Throughput Time*

Waktu menjalankan proses / *event* kadang memerlukan waktu lebih cepat atau lebih lambat dibanding dengan waktu standar. Waktu standard ditetapkan dari waktu dalam SOP ditambah waktu toleransi atas atau toleransi bawah. Sebuah proses / *event* yang dieksekusi lebih cepat dibanding waktu standard akan mengisi atribut *throughput min*, sedangkan jika waktu eksekusi event yang waktunya lebih lambat dibanding waktu standard akan mempengaruhi atribut *throughput time max*.

C. Analisis *Resource*

Analisis *resource* berfungsi untuk menganalisis adanya originator yang mengeksekusi *event* yang bukan wewenangnya. SOP mengatur bahwa originator dalam menjalankan sebuah *event* harus sesuai dengan level otoritas. Setiap *event* memiliki originator yang berhak menjalankannya. Sebuah *event* yang dijalankan oleh originator yang salah akan menghasilkan atribut *wrong resource*.

D. Analisis *Decision*

Analisis *Decision* berfungsi untuk menganalisis adanya pelanggaran pengambilan keputusan. Metode ini menganalisis originator yang menjalankan *event decision* sesuai dengan SOP atau tidak. Dalam SOP, sebuah *event* harus dieksekusi oleh originator yang memiliki otoritas.

E. Analisis *Segregation of Duty*

Analisis *Segregation of duty* ini digunakan untuk memeriksa adanya penyimpangan dalam pemisahan tugas. Penyimpangan terjadi, jika seorang originator menjalan dua atau lebih *event* yang berbeda dalam sebuah *case*. Analisis ini, biasanya digunakan di perusahaan besar. Penyimpangan *segregation of duty* berpengaruh pada atribut *wrong duty sequence* atau *wrong duty decision* atau *wrong duty combine*.

F. Analisis *Pattern*

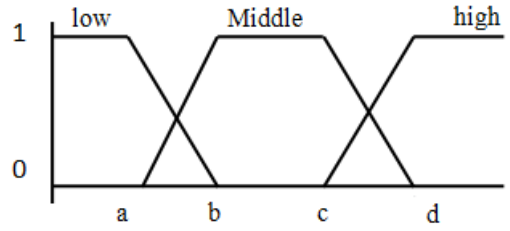
Metode analisis ini digunakan untuk menganalisis *flow* dari proses bisnis yang harus sesuai dengan pola model proses bisnis. Pola urutan eksekusi *event* yang tidak sesuai dengan SOP diidentifikasi sebagai pelanggaran. Pelanggaran pola berpengaruh pada atribut PBF yaitu atribut *wrong pattern*

G. Analisis *Event Parallel*

Analisis *event parallel* berfugsi untuk mengetahui terjadinya lebih dari satu event jalan secara bersamaan. Jika SOP mengharuskan *event-event* tersebut dijalankan secara berurutan, maka eksekusi event tersebut dianggap sebagai pelanggaran SOP. Pelanggaran SOP yang berupa menjalankan *event-event* secara bersamaan ini akan berpengaruh pada atribut *event parallel.*

Pembobotan *Attribute Value*

Attribute value adalah bobot pelanggaran yang terjadi dari sebuah atribut PBF. Untuk meningkatkan presisi dalam menentukan *attribute value* akan digunakan fuzzy. Fuzzy memiliki kemampuan untuk meningkatkan presisi [8]. Dalam penelitian ini, setiap *attribute value* diusulkan terdiri dari tiga fungsi keanggotaan dengan linguistik *low, middle* dan *high*. Bilangan fuzzy untuk masing-masing linguistik ditentukan berdasarkan pelanggaran yang pernah terjadi pada data *training*. Fuzzy ini menggunakan fuzzy trapezium, dimana keanggotaan untuk bobot atribut ditentukan sebagaimana dalam Gambar 2 [9].



Gambar 2. Keanggotaan fuzzy *Attribute Value*

Nilai *attribute value* berbeda antara bank satu dengan bank lainnya. Pakar anti fraud bank tersebut yang memahami kondisi low, middle dan high attribute value tersebut. Penelitian ini meminta pakar untuk menentukan nilai fuzzy dari masing-masing kondisi tersebut.

Pembobot Penting Atribut

Bobot penting atribut ditentukan oleh pakar dengan memberikan nilai penting atribut dibanding atribut lainnya. Metode *Modified Digital Logic* (MDL) untuk pembobotan atribut pernah digunakan dalam [10]. Penelitian ini juga menggunakan metode MDL untuk menentukan bobot penting atribut. Disini para pakar berdiskusi tentang penting atribut.

Empat pakar memberikan penilaian pentingnya atribut dibandingkan dengan atribut yang lain. Mereka menilai setiap atribut dengan '1', '2' atau '3'. Untuk menunjukkan bahwa atribut tersebut lebih penting menggunakan '3'. Untuk menunjukkan sama pentingnya menggunakan '2'. Sedangkan untuk kurang penting menggunakan '1'. Metode ini juga digunakan dalam [10].

Menghitung *Attribute Rating*

Attribute rating diperoleh dengan mencari *lower bound*, *middle weight* dan *upper bound* dari *attribute value* dan bobot penting atribut. Metode *decision vector* digunakan untuk memperoleh *attribute rating*.

Untuk menghitung *attribute rating* digunakan rumus 1.

$$(x_1, x_2, x_3, x_4) = (h_1 \times v_1, h_2 \times v_2, h_3 \times v_3, h_4 \times v_4) \quad (1)$$

dimana x_1 , x_2 , x_3 , x_4 adalah bilangan fuzzy dari *atribut rating*, h_1, h_2, h_3, h_4 adalah bilangan fuzzy dari *attribute value*, sedangkan v_1, v_2, v_3, v_4 adalah bilangan fuzzy bobot penting atribut. Rumus ini sudah digunakan dalam [11].

Menentukan Bobot PBF

Untuk menentukan bobot fraud digunakan rumus 2.

$$\mathcal{F} = S_1 \vee S_2 \vee S_3 \vee S_4 \vee \ldots \vee S_n \quad (2)$$

Dimana *S* attribute rating, *n* jumlah total atribut PBF dan $\mathcal{F}$ bobot PBF . Rumus ini digunakan dalam [11].

PEMBAHASAN

Kontribusi paper ini berupa penggunaan level event logs dalam mendeteksi PBF. Metode deteksi dalam penelitian sebelumnya [4,5,9] tidak dapat mengidentifikasi pelanggaran SOP yang berupa validasi KTP nasabah. Dalam kasus pembobolan bank lewat SMS banking, pelaku memanfaatkan celah kelemahan pada pendaftaran SMS

banking secara online. Keamanan SMS banking, sebetulnya sudah dirancang dengan validasi nasabah yang berupa validasi buku tabungan dan KTP nasabah. Validasi ini dilakukan untuk memperoleh fasilitas transaksi transfer dalam SMS banking. Saat ini pihak bank mempersilahkan nasabah mendaftarkan SMS banking secara online hanya untuk perolehan informasi tentang transaksi yang dilakukan. Namun untuk memperoleh firut transfer, pihak bank mensyaratkan nasabah harus datang ke cabang bank dimana mereka membuka rekening pertama kali. Selain itu, nasabah diwajibkan membawa KTP dan buku tabungan serta harus datang sendiri tidak boleh diwakilkan.

Dari beberapa pembobolan bank lewat SMS banking terjadi karena BO melanggar SOP, dimana mereka memvalidasi fitur transaksi transfer tanpa kedatangan ke kantor cabang bank. Pelanggaran SOP jenis ini tidak dapat dilakukan oleh metode deteksi fraud sebelumnya [9]. Paper ini mengusulkan level event logs untuk mendeteksi pelanggaran SOP jenis ini.

Dalam validasi nasabah, staf BO akan mencocokkan antara KTP, nasabah dan buku tabungan. Untuk implementasi metode kami mengajukan, event pengambilan data digital KTP nasabah disimpan dalam level 3 event logs. Kemudian event pencocokan foto nasabah dengan foto yang ada di KTP disimpan dalam event logs level 2. Terakhir event validasi nasabah disimpan dalam event logs level 1. Dalam setiap event logs masing-masing level disimpan informasi tambahan tentang validasi foto baru, kesamaan foto nasabah dengan KTP dan hasil validasi yang diperoleh.

Dalam case 5331, originator jena, melakukan validasi KTP pada nasabah dina.

Pada event logs level 1 tertulis 5331, 60101, aktifkan transfer, 19/11/2015:10:10:15, 19/11/2015;10:30:00,ya, Pada event log level 2 tertulis : 5331, 60101, perbandingan foto, 19/11/2015:10:12:10, 19/11/2015:10:15:15,true, Pada event logs level 3 tertulis 5331, 60101, pengambilan foto, 19/11/2015:10:10:12, 19/11/2015:10:10:00,yes.

Dalam analisis proses bisnis, case 5331 dibandingkan dengan sop. Pertama sistem akan membandingkan semua event dalam case 5331 menggunakan analisis skip. Pada event 60101, metode ini akan mengecek informasi validasi “ya”. Selanjutnya, metode ini menggunakan kunci 5331 dan 60101, metode ini mencari informasi pada event logs level 2. Hasil pencarian tersebut memperoleh informasi true, yang berarti mirip antara foto dengan foto nasabah dalam KTP. Terakhir metode ini membuka event logs level 3 dan memperoleh informasi yes, yang berarti documen foto tersebut baru diambil.

Analisis proses bisnis dilanjutkan menggunakan menggunakan analisis throughput time, analisis duty, analisis resource, analisis decision dan analisis event parallel. Hasil analisis tersebut menjadi dasar penentuan attribute value.

Berdasarkan attribute value, metode ini menentukan attribute ratin g menggunakan rumus (1). Terakhir menggunakan rumus (2) akan di tentukan bobot fraud. Dari data testing, 12 pelanggaran SOP berupa validasi nasabah transaksi SMS banking teridentifikasi. Penggunaan level event logs ini dapat mendeteksi fraud lebih akurat.

Pada penelitian selanjutnya hasil penelitian ini akan di gabungkan dengan metode deteksi fraud [11] sehingga metode fraud tersebut dapat diimplementasikan untuk deteksi fraud yang terjadi di SMS banking.

SIMPULAN DAN SARAN

Simpulan

Rancangan level *event logs* terbukti dapat memberikan informasi tentang validasi data. Level *event logs* ini diimplementasikan pada metode analisis *skip*. Dari semua case yang tidak melakukan validasi data dapat terdeteksi oleh level *event logs* ini.

Saran

Level event logs merupakan penelitian metode deteksi fraud pada SMS banking. Penelitian berikutnya akan menguji metode ini dalam kasus internet banking.

DAFTAR PUSTAKA

[1] Ngai, E.W.T., Hu, Y., Wong Y.H., Chen, Y. & Sun, X., *The Application of Data Mining Techniques in Financial Fraud Detection: A Classification framework and an Academic Review of Literature,* Decision Support Systems, **50**(3), pp. 559-569, 2010.

[2] Amara, I., Amar, A.B., Jarboui, A., *Detection of Fraud in Financial Statements: French Companies as a Case Study*, International Journal of Academic Research in Accounting, Finance and Management Sciences, **3**(3), pp. 44-55, 2013.

[3] Jans, M., van der Werf, M.J., Lybaert, N. & Vanhoof, K., *A Business Process Mining Application for Internal Transaction Fraud Mitigation*, Expert Systems with Applications, **38**(10), pp. 13351-13359, 2011.

[4] Stoop, J.J., *Process Mining and Fraud Detection*, Thesis, Business Information Technology Department, Twente University, Enschede, Netherlands, 2012.

[5] Dewandono, D.R., *Process Sequence Mining For Fraud Detection Using CEP*, Thesis, Informatics Department, Institut Teknologi Sepuluh Nopember, Surabaya, 2013.

[6] Sarno, R., Dewandono, D.R. Ahmad, T., Naufal, M.F. & Sinaga, F., *Hybrid Association Rule Learning and Process Mining for Fraud Detection*, IAENG International Journal of Computer Science, **42**(2), pp. 59-72, 2015.

[7] Huda, S., Sarno, R., Ahmad, T. & Santoso, H.A., *Identification of Process-based Fraud in Credit Application*, 2014 2nd International Conference on Information and Communication Technology (ICoICT), Telkom University, Bandung, Indonesia, pp. 84-89, 2014.

[8] Zadeh, L.A., *Fuzzy Sets*, Information and Control, **8**(3), pp. 338-353, 1965.

[9] S. Huda, R. Sarno and T. Ahmad, "*Fuzzy MADM approach for Rating of Process-based Fraud*", Journal ICT. Research Application, vol. 9, no. 2, **(2015)**, pp. 111-128.

[10] Vats, S., Vats, G., Vaish, R. & Kumar, V., *Selection of Optimal Toll Collection System for India : A Subjective-Fuzzy Decision Making Approach*, Applied Soft Computing, **21**, pp. 444-452, 2014.

[11] S. Huda, R. Sarno and T. Ahmad., "*Increasing Accuracy of Process-based Fraud Detection Using a Behavior Model"*, International Journal of Software Engineering and Its Applications, **10**(5), pp. 175-188, 2016.

Tabel 1. Atribut PBF

Atribut	Deskripsi
Skip sequence	*Skip* pada *event sequence* yaitu *event* yang terarah pada satu *event* berikutnya
Skip decision	*Skip* yang terjadi pada *event* yang memiliki percabangan
Througput time min	Waktu eksekusi *event* yang nilainya lebih kecil dari nilai standard *event*

Througput time max	Waktu eksekusi *event* yang nilainya lebih besar dari nilai standard *event*
Wrong resource	*Event* yang dieksekusi oleh originator yang berwenang
Wrong duty sequence	*Event* yang dieksekusi oleh originator yang mengeksekusi lebih dari satu *event* pada *event sequence*
Wrong duty decision	*Event* yang dieksekusi oleh originator yang mengeksekusi lebih dari satu *event* pada *event decision*
Wrong duty combine	*Event* yang dieksekusi oleh originator yang mengeksekusi lebih dari 1 *event* pada *event decision* dan *sequence*
Wrong pattern	*Case* yang polanya berbeda dengan SOP
Wrong decision	*Event* yang memiliki keputusan yang tidak sesuai dengan SOP
Events parallel	Eksekusi *event* secara bersamaan dan melanggar SOP