Finite-state automata modeling pattern of systems-theoretic process analysis results

RAMS Seminar
Date: Thursday 18.03.2021
By Nanda Anugrah Zikrullah
Outline

1. Introduction
2. Study case
3. Discussion
Introduction
From previous work

Integration concept

Systems-Theoretic Process Analysis

STPA – Generated requirements

- Example of unsafe control actions (UCA): MCS provides \( \text{aut. command pump shutdown} \) to PSD node when scrubber level status is normal and the pump status is running / unknown [LSc093-103]

- Example of controller constraints (CC):
  - MCS must not provide \( \text{aut. command pump shutdown} \) to PSD node when scrubber level status is low and the pump status is running / unknown [LSc093-103]

Unsafe control actions (Hazards) & Safety requirements
Systems-Theoretic Process Analysis

• Hazard analysis technique developed by Leveson
• Based on systems theory and systems thinking
• Utilize a control structure model
Why STPA?

STPA
- Inadequate coordination
- Interaction problem
- Unsafe decision making

HAZOP
- Software requirement error
- Process design error

FMEA
- Component failure
Problem formulation and available contributions

• How can STPA results be used in a decision-making context?
  – Zikrullah et al. (2021) – Generate high-level safety requirements
  – Kim et al. (2020) – Risk-based prioritization of safety measures
  – Zhang et al. (2019) – Incorporating results from STPA into availability calculation
  – Our contribution (under progress) – Incorporating results from STPA to support safety demonstration
Finite state automata (FSA)

- An approach to model the system as a set of finite states
- Used to quantify system availability or mean time to failures
- Example techniques:
  - Markovian
  - Petri nets
  - Textual-based formal language (e.g., Altarica 3.0)
STPA-FSA modeling approach
Examples of STPA result

UCA example:

• UCA001. Controller xxx does not provide control action xxx to the controlled process during the condition xxx [H1]
UCA classification

Classification of UCAs:
1.) not providing the control action during a specific condition,
2.) providing unnecessary control action (leading to hazard),
3.) providing a potentially safe control action but too early, too late, or in the wrong order,
4.) the (continuous) control action lasts too long or is stopped too soon.
(Generic) Controlled process model

UCA Type 1
Examples of STPA result

Loss scenario example:

• LSc001. Coupling of hardware failure in component xxx and systematic failure in component xxx results into UCA001.
Loss scenario classification

- Loss scenarios
  - (Removable) loss scenarios
    - Classification
      - Removed by system design
    - Solution
      - Systematic treatment to control scenario's occurrence
  - (non-removable) loss scenarios
    - Classification
      - (non-quantifiable) loss scenarios
    - Solution
      - Quantification of scenarios' risk based on RAM framework followed by risk reduction treatment

Numbers:
- 1
- 2a
- 2b
(Generic) Control element model for single failure type

I. Single failure
   1. Random hardware failure (RHF)
      a) Detected
      b) Undetected
   2. Systematic failure
      a) Software
         i. Multiple occurrence. Reappearance follows a stochastic behavior
         ii. Single occurrence. Can be removed by system design (cannot be modelled)
      b) Human (the occurrence follows a stochastic behavior)
Control element model for multiple failure type

I. Multiple failure
   1. Common cause failure
   2. Cascading failure -> Utilize combination of single failure type model
Study case
Subsea compression system schematic
Example of STPA results

• UCA22. SS part of the logic solver must provide Shutdown equipment command to SS actuator when the gas temperature is very high and the compressor is running [H2]

• Loss scenarios list:

<table>
<thead>
<tr>
<th>LSID</th>
<th>Scenario</th>
<th>Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS104</td>
<td>Erroneous information from the SS sensor results in inaccurate information processed at the controller</td>
<td>2b</td>
</tr>
<tr>
<td>LS105</td>
<td>Component failure of the SS actuator results in system inability to process the control command</td>
<td>2b</td>
</tr>
<tr>
<td>LS106</td>
<td>Component failure of the SS sensor results in inaccurate information processed at the controller</td>
<td>2b</td>
</tr>
<tr>
<td>LS107</td>
<td>Problem in the transmitted information (e.g., erroneous, delay) results in inability to transfer information/command in the control loop</td>
<td>2a</td>
</tr>
<tr>
<td>LS108</td>
<td>Component failure of the communication transmission system results in inability to transfer information/command in the control loop</td>
<td>2b</td>
</tr>
<tr>
<td>LS109</td>
<td>Algorithm flaw on the SS part of the logic solver is a design problem that cause unintended functionality at the controller</td>
<td>1</td>
</tr>
<tr>
<td>LS110</td>
<td>Component failure of the PCS/SS logic solver (shared) results in incorrect administration of control action</td>
<td>2b</td>
</tr>
<tr>
<td>LS111</td>
<td>Unintended overwrite from PCS to SS in the logic solver is a design problem that cause unintended functionality at the controller</td>
<td>2a/2b*</td>
</tr>
<tr>
<td>LS112</td>
<td>Resource sharing problem between PCS and SS in the logic solver is a design problem that cause unintended functionality at the controller</td>
<td>1</td>
</tr>
</tbody>
</table>

* Depending on data availability
Loss scenario classification

- **Loss scenarios**
  - (Removable) loss scenarios
  - (non-removable) loss scenarios
    - (non-quantifiable) loss scenarios
      - Systematic treatment to control scenario’s occurrence
    - (quantifiable) loss scenarios
      - Quantification of scenarios’ risk based on RAM framework followed by risk reduction treatment

Solution

1. Removed by system design
2a. Systematic treatment to control scenario’s occurrence
2b. Quantification of scenarios’ risk based on RAM framework followed by risk reduction treatment
Scenario’s modeling

UCA example:
• UCA22. SS part of the logic solver must provide Shutdown equipment command to SS actuator when the gas temperature is very high and the compressor is running [H2]

Loss scenario example:
• LS110. Component failure of the PCS/SS logic solver (shared) results in incorrect administration of control action
• LS111. Unintended overwrite from PCS to SS in the logic solver is a design problem that cause unintended functionality at the controller
Source code for implementation

- Altarica 3.0
  - Library module for controlled process model and control element models
Results (Stepwise simulation)

For verification of system behavior
### Parameters for simulation (from PDS (2021) and experts judgment)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Probability distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS Sensor failure rate</td>
<td>DU = 2e-7 /hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>SS Sensor erratic reading rate</td>
<td>DD = 4e-7 /hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>SS Actuator failure rate</td>
<td>DU = 5e-7 /hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Communication equipment failure rate</td>
<td>DD = 1e-8 /hour (assumption, need discussion)</td>
<td>Exponential</td>
</tr>
<tr>
<td>PCS/SS logic solver failure rate</td>
<td>DU = 1.1e-6 /hour; DD = 1.5e-6 /hour</td>
<td>Exponential Exponential</td>
</tr>
<tr>
<td>SS software systematic fault introduction rate</td>
<td>Sys= 1e-8 /hour (assumption, need discussion)</td>
<td>Exponential</td>
</tr>
<tr>
<td>Repair time</td>
<td>8 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Repair delay</td>
<td>8 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Inspection period</td>
<td>once every 6 months</td>
<td>Dirac</td>
</tr>
<tr>
<td>Inspection duration</td>
<td>24 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Frequency of context change</td>
<td>once per year</td>
<td>Exponential</td>
</tr>
<tr>
<td>System restoration time</td>
<td>8 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Simulation time</td>
<td>87,600 hour</td>
<td>n/a</td>
</tr>
<tr>
<td>Number of simulations</td>
<td>500,000</td>
<td>n/a</td>
</tr>
</tbody>
</table>
# Results (Stochastic simulation)

<table>
<thead>
<tr>
<th>meta-data</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>number of runs</td>
<td>500000</td>
<td></td>
</tr>
<tr>
<td>seed</td>
<td>12345</td>
<td></td>
</tr>
<tr>
<td>mission-time</td>
<td>87600.0</td>
<td></td>
</tr>
<tr>
<td>model-name</td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>file-name</td>
<td>C:/Users/nandao/Google Drive/RAMS/PhD/Research/Altairca/Juntao/System.gts</td>
<td></td>
</tr>
<tr>
<td>start-time</td>
<td>Tue Feb 15 12:48:22 2021</td>
<td></td>
</tr>
<tr>
<td>end-time</td>
<td>Tue Feb 16 12:48:22 2021</td>
<td></td>
</tr>
<tr>
<td>steps min</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>steps mean</td>
<td>22.6083</td>
<td></td>
</tr>
<tr>
<td>steps max</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td>tool version</td>
<td>2.0.0</td>
<td></td>
</tr>
<tr>
<td>compiler version</td>
<td>2.0.0</td>
<td></td>
</tr>
</tbody>
</table>

**Observer SCA22**
- Type: Boolean
- Number of occurrences: 500000
- Value: True
- Mean: 2.03858
- Standard-deviation: 1.49259
- Confidence-interval: [0.95, 0.05] size: [0.001452, low: 2.0452, high: 2.04352]

**Observer UCA22**
- Type: Boolean
- Number of occurrences: 500000
- Value: True
- Mean: 0.474194
- Standard-deviation: 0.471913
- Confidence-interval: [0.95, 0.05] size: [0.001794, low: 0.472475, high: 0.475913]

**Observer Ufailure**
- Type: Integer
- Value: 0.717696
- Standard-deviation: 0.70462
- Confidence-interval: [0.95, 0.05] size: [0.001953, low: 0.715743, high: 0.719649]
## Result tabulation

<table>
<thead>
<tr>
<th>Loss scenario ID (Causal factor)</th>
<th>LS frequency (/year) (Individual simulation)</th>
<th>Simulation time</th>
<th>LS frequency (/year) (Combined simulation)</th>
<th>Simulation time</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS104 (Sensor)</td>
<td>3.780E-04</td>
<td>9 s</td>
<td>3.778E-04</td>
<td>-</td>
</tr>
<tr>
<td>LS105 (Actuator)</td>
<td>9.342E-04</td>
<td>9 s</td>
<td>9.198E-04</td>
<td>-</td>
</tr>
<tr>
<td>LS106 (Sensor)</td>
<td>8.200E-06</td>
<td>8 s</td>
<td>1.260E-05</td>
<td>-</td>
</tr>
<tr>
<td>LS108 (Communication)</td>
<td>6.000E-07</td>
<td>8 s</td>
<td>4.000E-07</td>
<td>-</td>
</tr>
<tr>
<td>LS110 (PCS/SS logic Solver)</td>
<td>2.102E-03</td>
<td>18 s*</td>
<td>2.073E-03</td>
<td>-</td>
</tr>
<tr>
<td>LS111 (PCS/SS logic Solver)</td>
<td>7.600E-05</td>
<td>9 s</td>
<td>8.280E-05</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total UCA frequency &amp; simulation time</strong></td>
<td>3.499E-03 (avg. 60.86 s)</td>
<td>3.460E-03 (avg. 27.27 s)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* two simulations are performed due to contribution from several causal factors (undetected & detected failure)
Sensitivity analysis

Sensitivity analysis results for individual simulation

Sensitivity analysis results for combined simulation
Discussion
Contribution of the new approach

- Capability to model systematic faults
- Aggregation of multiple scenarios into one model (for LSs)
- Improved simulation time
- Comparison with traditional quantitative modeling approach
- Prioritization based on quantified value
- Reduction of model uncertainty
- Input for risk assessment method using STPA
Capability to model systematic faults
Combined simulation results

<table>
<thead>
<tr>
<th>Loss scenario ID (Causal factor)</th>
<th>LS frequency (/year) (Individual simulation)</th>
<th>Simulation time</th>
<th>LS frequency (/year) (Combined simulation)</th>
<th>Simulation time</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS104 (Sensor)</td>
<td>3.780E-04</td>
<td>9 s</td>
<td>3.778E-04</td>
<td>-</td>
</tr>
<tr>
<td>LS105 (Actuator)</td>
<td>9.342E-04</td>
<td>9 s</td>
<td>9.198E-04</td>
<td>-</td>
</tr>
<tr>
<td>LS106 (Sensor)</td>
<td>8.200E-06</td>
<td>8 s</td>
<td>1.260E-05</td>
<td>-</td>
</tr>
<tr>
<td>LS108 (Communication)</td>
<td>6.000E-07</td>
<td>8 s</td>
<td>4.000E-07</td>
<td>-</td>
</tr>
<tr>
<td>LS110 (PCS/SS logic Solver)</td>
<td>2.102E-03</td>
<td>18 s*</td>
<td>2.073E-03</td>
<td>-</td>
</tr>
<tr>
<td>LS111 (PCS/SS logic Solver)</td>
<td>7.600E-05</td>
<td>9 s</td>
<td>8.280E-05</td>
<td>-</td>
</tr>
</tbody>
</table>

Total UCA frequency & simulation time

<table>
<thead>
<tr>
<th>Failure rate value</th>
<th>Individual Contribution</th>
<th>Effect to UCA</th>
<th>Individual frequency (with base value)</th>
<th>Simulation Time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS104 (Sensor DU) -50%</td>
<td>1.000E-07</td>
<td>1.810E-04</td>
<td>3.315E-03</td>
<td>n/a</td>
</tr>
<tr>
<td>LS104 (Sensor DU) base</td>
<td>2.000E-07</td>
<td>3.778E-04</td>
<td>3.460E-03</td>
<td>3.778E-04</td>
</tr>
<tr>
<td>LS104 (Sensor DU) +50%</td>
<td>3.000E-07</td>
<td>5.620E-04</td>
<td>3.667E-03</td>
<td>n/a</td>
</tr>
</tbody>
</table>

* two simulations are performed due to contribution from several causal factors (undetected & detected failure)
Improved simulation time (?)

Comparison with Zhang et al. (2019)

<table>
<thead>
<tr>
<th>Failure rate (/hour)</th>
<th>Juntao’s result (UCA freq./year)</th>
<th>Simulation time</th>
<th>My result (UCA freq./year)</th>
<th>Simulation time</th>
</tr>
</thead>
<tbody>
<tr>
<td>5e-6</td>
<td>3.3e-4</td>
<td>~44 minutes</td>
<td>2.5e-2</td>
<td>3 seconds</td>
</tr>
<tr>
<td>1e-5</td>
<td>5.7e-4</td>
<td>~44 minutes</td>
<td>4.7e-2</td>
<td>3 seconds</td>
</tr>
<tr>
<td>1.5e-5</td>
<td>7.9e-4</td>
<td>~44 minutes</td>
<td>6.6e-2</td>
<td>3 seconds</td>
</tr>
</tbody>
</table>

• Differences in the result are caused by several reasons:
  – Unseen parameters from Juntao’s paper
  – Transition that are coupled between LS 1 and 2 in the Juntao’s model (not modelled due to missing information)
Comparison with traditional quantitative modeling approach

• STPA-FSA approach is essentially quantifying PFH and demand rate in the same model

STPA-FSA approach

IEC 61508 approach

Systematic failure

Random hardware failure
Prioritization based on quantified value
Reduction of model uncertainty
Input for risk assessment method using STPA (Kim, 2020)

Table 4. Evaluation criteria for loss scenarios.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Category and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood* (LH)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Event that is expected to occur frequently.</td>
</tr>
<tr>
<td></td>
<td>4. Event that happens now and then and will normally be experienced by the personnel.</td>
</tr>
<tr>
<td></td>
<td>3. Rare event, but will possibly be experienced by the personnel.</td>
</tr>
<tr>
<td></td>
<td>2. Very rare event that will not necessarily be experienced in any similar plant.</td>
</tr>
<tr>
<td></td>
<td>1. Extremely rare event.</td>
</tr>
<tr>
<td>Strength of knowledge on loss scenario (SOK)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Complex scenario with no or few experience.</td>
</tr>
<tr>
<td></td>
<td>4. Complex scenario with a small number of experiences.</td>
</tr>
<tr>
<td></td>
<td>3. Complex scenario with a large number of experiences.</td>
</tr>
<tr>
<td></td>
<td>2. Straightforward scenario with a small number of experiences.</td>
</tr>
<tr>
<td></td>
<td>1. Straightforward scenario with a large number of experiences.</td>
</tr>
</tbody>
</table>

*R For details of classifications of likelihood, readers can refer to Rausand.\(^{(29)}\)

\[ RPN_{LossScenario} = RPN_{UCA} \times LH \times SOK_{LossScenario} = SV \times ATR \times SOK_{ECA} \times LH \times SOK_{LossScenario} \]
Approach limitation

• Data uncertainty
• Completeness uncertainty
• Aggregation of multiple scenarios into one model (for UCAs)
# Data uncertainty

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Probability distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS Sensor failure rate</td>
<td>DD = 2.490e-8 /hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>SS Sensor erratic reading rate</td>
<td>DU = 2.122e-7 /hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>SS Actuator failure rate</td>
<td>DU = 3e-7 /hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Communication equipment failure rate</td>
<td>DD = 1e-6 /hour (assumption, need discussion)</td>
<td>Exponential</td>
</tr>
<tr>
<td>PCS/SS logic solver failure rate</td>
<td>DU = 3.810e-8 /hour; DD = 4.25e-7 /hour</td>
<td>Exponential Exponential</td>
</tr>
<tr>
<td>SS software systematic fault introduction rate</td>
<td>Sys= 5e-6 /hour (assumption, need discussion)</td>
<td>Exponential</td>
</tr>
<tr>
<td>Repair time</td>
<td>8 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Repair delay</td>
<td>8 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Inspection period</td>
<td>once every 6 months</td>
<td>Dirac</td>
</tr>
<tr>
<td>Inspection duration</td>
<td>24 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Frequency of context change</td>
<td>once per year</td>
<td>Exponential</td>
</tr>
<tr>
<td>System restoration time</td>
<td>8 hour</td>
<td>Exponential</td>
</tr>
<tr>
<td>Simulation time</td>
<td>87,600 hour</td>
<td>n/a</td>
</tr>
<tr>
<td>Number of simulations</td>
<td>100,000</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Completeness uncertainty

STPA-FSA steps

STPA steps

Step 1: Define the purpose of the analysis

Step 2: Model the control structure

Step 3: Identify unsafe control actions (UCA)

Step 4: Identify loss scenarios

Step 5: Classify STPA results

Step 6: Model STPA results
Aggregation of multiple scenarios into one model (for UCA)

Loss scenarios

(Removable) loss scenarios

(non-removable) loss scenarios

Classification

Solution

Removed by system design

Systematic treatment to control scenario’s occurrence

Quantification of scenarios’ risk based on RAM framework followed by risk reduction treatment

Omission of some scenario’s risk
References


[4] M. Rodriguez, F. Diya, A systematic and integral haz-


ation of the FMVA and NITA safety analysis methods—
Reference

[7] R. Rokne, J. D. Urquhart, Deriving veri-


[12] J. Zhang, H. Kim, Y. Lin, M. A. Lundteigen, Com-
ining system-theoretic process analysis and availabil-


[15] H. Mags, L. Khou, A. Rausch, Modeling patterns for re-
liability assessment of safety instrumented systems, Re-

[16] ISO/TR 12495, Petroleum, petrochemical and natural


[18] M. Batteux, T. Provostvann, A. Rausch, Modelling pat-
terns for the assessment of maintenance policies with altitudes 3.0, in: International Symposium on Model-


[22] A. Toola, The safety of process automation, Automat-
as 29 (2009) 541-548.

[23] I. Xie, M. Lundteigen, Y. Liu, Safety barriers against common causes failure and cascading failure. Literature review and a novel modeling system, in: 2018 IEEE International Con-
nference on Industrial Engineering and En-
gineering Management (IEEM), IEEE, 2018, pp. 122-
127.


[27] J. i. Aparna, R. Menlak, Model-based design of de-


[29] IEC 62551, Analysis techniques for dependability − Petri net techniques, Standard, International Elec-


[32] R. Babuschkin, Agent-based and individual-

[33] O. Nyitrai, S. Huang, L. Perki, Complex accident scenar-
io models and analysed by stochastic petri nets, Re-
liability Engineering & System Safety 142 (2015) 539-
550.

[34] J. P. Sgionve, Y. Davit, P. J. Cachery, C. Hifke,
S. Colbre, P. Thomas, Make your petri nets understand-
able: Reliability block diagrams driven petri nets, Re-
liability Engineering & System Safety 113 (2013) 61-75.

[35] Qi. Wen, D. Geemy, F. Hubert, E. Laveur, Towards a model-based systems engineering (mbe) pattern to ef-

ciently reuse know how, Insight 20 (4) (2017) 31-33.

[36] H. Ilam, J. Perez, Supporting pattern-based depend-
ability engineering via model-driven development: Ap-

[37] D. Cook, W. D. Schindel, Utilising mbe patterns to accelerate system verification, Insight 20 (1) (2017) 32-
41.

[38] N. A. Zikerallah, M. J. P. van der Meulen, M. A. Lund-
teigen, A Comparison of hazard analysis methods for capability safety requirements generation, Proceedings of the Institution of Mechani-


[40] N. A. Zikerallah, M. J. P. van der Meulen, M. A. Lundteigen, Building blocks for safety argumentations with sipas, in: XXX, XXX, XXX, XXX.

[41] J. F. Thomas, Fourth, Extending and automating a systemso-


[43] INVELEP-A20 technology qualification, Recom-
mendation.


[45] R. K. NAON, A guide to practical human reliability as-

[46] N. A. Zikerallah, M. J. P. van der Meulen, G. Skofte-
land, M. A. Lundteigen, Systemic technology process anal-

[47] INVELEP-BA4, Safety 4.0, retrieved 2021-09-10. URL : https://www.invelep.com/research/all-

[48] Recommended practice for analysis, design, installa-
tion, and testing of safety systems for nuclear applica-

Thank you