Real-Time Root Cause Analysis for Complex Technical Systems

Jan Eric Larsson, Joseph DeBor

IEEE HPRCT
Monterey, CA, August 29th 2007
Handling Alarm Cascades

Root cause analysis: find the initiating events in a complex fault situation
GoalArt’s Solution

• We provide
  – Software system
  – For *industrial plants* and *complex technical products*
  – Helps operators understand current fault situation
  – In unexpected and dangerous situations
  – Quick and correct actions

• Benefits
  – Increased availability
  – Less downtime
  – Efficient diagnosis and repair
  – Less risk for large blackouts
  – Better environment for operators

Power plant control room
Customers

ABB
Control systems
Nuclear power
Medical equipment
Power and heating
Power and heating
Power grid research
Power grid
Nuclear power

Barsebäck
Power grid

Dräger Medical
Power grid
Medical equipment

Elsam
Nuclear power
Elsam Engineering
Power and heating

EPR1
Power grid research

FirstEnergy
Power grid
Forsmarks Kraftgrupp
Nuclear power

Fortum
Power grid

Gambro
Vallviks Bruk

Institute for Energy Technology
Power grid

Jönköping ENERGI
Nuclear research

Lund Energy
Power and heating

Midwest ISO
Power grid

Power grid

ISO
Nuclear power

Ringhals
Power and heating

TVO
Power grid

Svenska Kraftnät
Nuclear power

Sydkraft
Power and heating

Vallviks Bruk
Nuclear power

Vattenfall
Vehicles

Volvo Bus
Pulp and paper research

Åforsk
Pulp and paper
Multilevel Flow Models

- Multilevel Flow Models (MFM)
- Formal graphical representation with high abstraction level
- Well established and tested from research
- Describes goals and functions of industrial systems
  - Goals: why do we run the system
  - Functions: the capabilities of the system
- Functions describe flows of mass, energy, and information
- Describes to the process should work and not fault situations!
  - Much less modeling work, handles unpredicted situations
- Most algorithms based on one single model
- Good real time properties, enables fast algorithms
Multilevel Flow Models

- Line 1 trips from internal fault
- Line 2 overloads
- Analysis
  - Line 1 is a root cause
  - Line 2 is a consequence
- Root cause analysis can reduce large alarm cascades to single root cause alarms
How Does It Work?

- Simple example
  - Pump and closed tank
- Described as transport and storage
- Four consequence propagation rules are valid for this connection
Simple Cases
Principal Algorithm

- Consequence propagation rules defined for each legal MFM connection
- Diagnostic state is updated incrementally as new observations come in
- Look upstream and downstream to next observation only

- Gives low computational complexity
  - Typical case is constant, independent of model size / inputs / diagnoses
  - Worst case is linear in model size / inputs / diagnoses
  - Complete analysis of 200 000 input system takes ~ 50 milliseconds

- We have several “tricks” to make the algorithm useful in practice
  - Handle all types of loops and multiple root causes
  - Switch causations on and off
Simple Power Grid Example
Needed Tables
Example Situation Analysis
Presentation

- GoalArt provides information
  - Primary / consequences
  - Dynamic priority / suppression
  - Sensor faults

- Can be presented in different ways
  - Alarm lists
  - Process schematics
  - Text messages
  - Advanced graphics
  - Sound

- GoalArt can help with design
  - Some examples in demo
Vallvik 1998

- Pulp and paper plant
- Alarm cascade
  - Tube leak
  - > 100 alarms during first minute
  - Explosion ten minutes later
- GoalArt system
  - MFM model with 500 inputs
  - Built and tested in 4 days
  - Comprises entire boiler
- Result
  - Correctly identifies root cause alarms
  - There would have been time (!)
August 14, 2003

- Largest blackout in the world so far
- Started in First Energy area, Ohio
  - Three independent lines sagged into trees
  - “Electric vegetation management”
- Developed slowly 3:05 PM to 4:05 PM
- Large cascade over eastern US and Canada 4:05 to 4:15 PM
- Very costly
  - 50 million people
  - 61 800 MW
  - Up to 4 days to restore everything
  - Estimated 4 – 10 million USD
  - GDP down 0.7 % in Canada
Conclusions from August 14 Demo

- Independent problems
  - Three lines short-circuited
  - First Energy’s alarm system software stopped

- Root cause analysis would have helped to identify the overload
  - Three 345 kV lines tripped
  - Underlying 138 kV lines overloaded and tripped
  - More 345 kV lines tripped
  - When Sammis – Star tripped, the cascade became irreversible

- Time to avoid the blackout
  - The First Energy overload and trip development lasted 3:05 to 4:05
Nuclear Project

- Diagnostic station connected to training simulator
- Excellent results
- System size 6500 signals
- On-line real-time to training simulator
- Possible to visit / get reference
- Barsebäck, Forsmark, Oskarshamn, Ringhals, Loviisa, Olkiluoto
- Total of 15 reactors from 500 – 2000 MW
Knowledge Engineering

• Knowledge acquisition process
  – Major effort
  – Good documentation
  – Process expertise required
  – IFE Halden valuable source

• Model construction
  – Quite efficient
  – Large task because of number of signals

• Testing and correction
  – Large task
  – All systems must be tested at least once
  – Complex system needs simulator

• Formal testing and validation
  – Not done in this project

• Current model size
  – 6 500 signals used, of 9 600 total signals
  – 60 % of signals handled
  – 40 % of signals tested
  – 12 000 MFM objects
  – Largest MFM model ever built by hand

• Corresponding expert system
  – Alarm project demo: 50 000 – 70 000 rules
  – Authorizer’s Assistant: 35 000 rules
    • More than 100 man-years effort (!)
    • Five people for permanent maintenance
  – Toshiba’s largest system: 5 000 rules
  – We are already past the limit of world’s largest knowledge-based system
Hambo Simulator

- Developed at HAMMLAB, IFE Halden, Norway
- True model of Forsmark 3, largest Swedish BWR
- Around 9500 status indications
- Several uses
  - Operator training
  - HMI design
  - Human factors experiments
- Sponsored by all Scandinavian nuclear power plants
Hambo Overview
Computational Efficiency I

- Midwest ISO power grid
  - 21,400 stations, 32,300 lines, 230,000 signals, 42,000 faults
- Complete computation time ~ 1.4 seconds on standard PC (3 GHz)
- No other diagnostic method can handle this size of system
Computational Efficiency II

• Rule-based expert systems
  – Charles Forgy: RETE III, Blaze Advisor: 2.5 million RPS, 300 % faster than competitors
  – NASA SHINE: 230 million RPS according to Viaspace own press release
  – Fuzzy logic hardware chip design (research, Australia): 1.2 billion RPS

• Midwest ISO knowledge base corresponds to ~ 2.5 million rules
  – 230 000 signals => 2.5 million rules
  – 42 000 faults => 42 000 executions
  – Total calculation time ~ 3 seconds of CPU
  – \(2 \times 10^6 \times 42 \times 10^2 / 3 = 35 \times 10^8\)

• Apparent GoalArt rule speed 35 billion RPS
  – More than a factor of 100 – 10 000 compared to fastest rule-based systems?
Computational Efficiency III

- **Well-known large rule-based systems**
  - Toshiba electric power plant, largest technical expert system: 6 000 rules
  - American Express, Authorizer’s Assistant, (> 200 man-years): 30 000 rules
  - Classical forward or backward chaining

- **New, web-based or database-like systems**
  - OpenCYC, world’s largest general knowledge base, first version: 60 000 rules
  - OpenCYC, current version: > 1 000 000 “assertations”
  - World Wide Web?
  - No reasoning engines or algorithms for advanced diagnosis available

- **GoalArt knowledge bases**
  - Forsmark 3 nuclear power plant, largest hand-built (4 man-months): 65 000 rules
  - Midwest ISO, largest auto-generated power grid knowledge base: 2 500 000 rules
  - GoalArt root cause analysis algorithm
Integration

- GoalArt Diagnostic Station (GDS)
  - Reads data from control system
  - Performs diagnostic calculations
- GoalArt Engineering Station (GES)
  - Design and maintenance of models
  - Configuration of GDS
- Standard interfaces
  - OPC for alarm and event data
  - CIM for grid topology
- Benefits
  - Well-defined interface to control system
  - Minimal changes in control system
  - Safe, because control system is not affected
Blackout September 23rd, 2003

- Large blackout in Scandinavia
- September 23rd 2003, 12.35 PM
- Root causes
  - 12:30 OKG 3 nuclear reactor trip (east)
  - 12:35 Internal station short-circuit (west)
- Consequences
  - Two lines for all of southern Sweden
  - Southern Sweden collapsed (5-15 min)
  - Eastern Denmark collapsed
  - Lasted 1-5 hours
- Actions
  - Second root cause unknown for 4 hours
  - Helicopters looking for line faults
- Cost
  - Lost ~ 10 000 000 kWh
  - Cost ~ 500 000 000 USD
  - Largest disturbance in 20 years
GoalArt Demo of Sep 23 Blackout

- **Demo contains**
  - Auto-generated MFM model from Oracle databases
  - Alarm cascade from control system
  - Covers all main events
  - Time order is approximately correct
  - Some alarms arrive in wrong order

- **Demo does not contain**
  - No alarm grouping/filtering

- **Conclusions**
  - The cascade is correctly analyzed
  - No manipulation of MFM model needed
  - Proof of concept on real system
  - Commercial delivery now ongoing
Presentation

- GoalArt provides information
  - Primary / consequences
  - Dynamic priority / suppression
  - Sensor faults
- Can be presented in different ways
  - Alarm lists
  - Process schematics
  - Text messages
  - Advanced graphics
  - Sound
- GoalArt can help with design
  - Some examples in demo
Summary

- Alarm cascades tend to obliterate situation awareness
- This happens exactly when larger incidents develop
- Root cause analysis can solve this problem
  - Makes the alarm system useful during incidents
- Now there is a new technology for root cause analysis
- Plug-and-play solution

a realistic solution for alarm cascades