

[invited]

High-Level Situation Management in Dynamic Networks and Systems

**Dr. Gabriel Jakobson, Chief Scientist
Altusys Corporation
www.altusystems.com**

Keywords: network management, dynamic systems, ad hoc mobile networks, tactical battlespace management, situation awareness, situation management, event correlation, distributed systems,

Altusys Corporation

Towards New Generation of Dynamic Networks and Systems

- Over the last decade we have witnessed introduction of new types of networks and systems characterized by
 - Large-scale distribution of the system components
 - Ad hoc and unpredictable changes in the system configuration
 - Introduction of new types of relations between components, including spatial, temporal, causal, and other domain-specific relations
 - High mobility of components
 - Weaker centralized control authority
 - Operational change in the functional role of the components
 - Higher autonomy, automatic operations, and self-organization of the nodes
- Examples of those systems include
 - Network-centric and asymmetric tactical battlefields,
 - Sensor and hoc mobile networks,
 - Homeland security and emergency/crisis management,
 - real-time applications in medical and financial services, and others;
- Central to understanding the behavior of these systems are
 - situations and
 - situation management.

Altusys Corporation

1

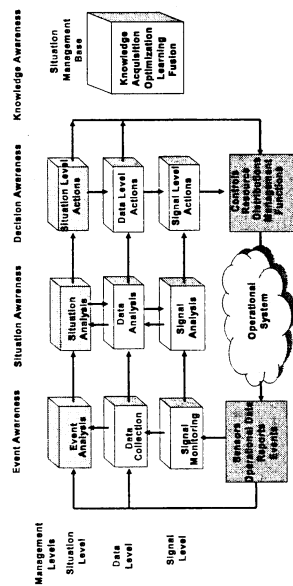
Basic Principles of Situation Management

- Informally, situations are defined as states of a system considered at specific time;
- Complexity of the situations may range from
 - a single attribute value, or a single relation among the attribute values
 - to states of large collections of objects interlinked by various spatial, temporal, structural, causal, and other domain-specific relations;
- Situation management is considered as a continuous process of
 - Instrumenting the system and the surrounding domain
 - modeling the system topology and dynamic behavior
 - tracking, predicting, planning, and controlling of situations
 - acting upon it so that the management goals are achieved;
- We will identify significant types of situation management, including
 - diagnostic type of situation management
 - control type of situation management
 - predictive type of situation management
 - explanation type of situation management

Altusys Corporation

2

Generalized Situation Management Model



Altusys Corporation

3

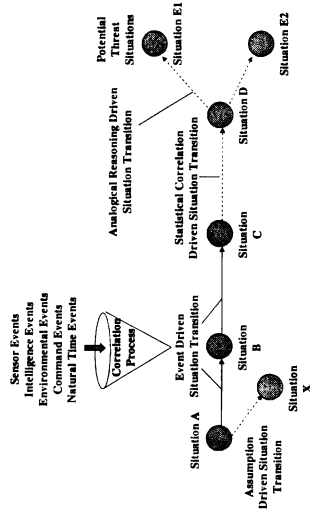
Basic Function Associated with Situation Management

- Event Awareness**
 - Primary data collection, filtering
- Situation Awareness**
 - Fusion of multi-source data
 - Understanding meaning of data, recognizing complex time-dependent patterns, and construction of situation models
 - Determining threats, intrusions, hostile activities, system failures, and activities that reveal intent or capability
- Decision Awareness**
 - Reasoning about situations, planning alternative action-oriented decisions, and implementing selected actions
 - Informing, and advising human operators (commanders) on the content and ramifications of the suggested actions
- Knowledge Awareness**
 - Mining historic operational data, generating new fusion patterns, discovery of new situation classes
 - Learning and improving the effectiveness of fusion procedures, situation analysis, and decision-making procedures

Altusys Corporation

4

Situation Modeling Using Situation Transition Graphs (STG)



Altusys Corporation

5

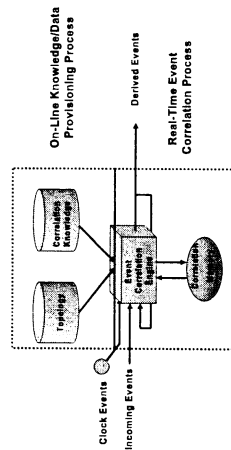
Situation Management Based on Real-Time Event Correlation

- Event Correlation as a branch of Computer Science and Information Technology has been a focus of extensive research and practical applications over the last 15 years
- Conceptually, Event Correlation is a real-time event analysis procedure, which assigns new meaning to the set of discovered events
- Practically, it is a software platform that enables real-time management of complex networks and systems, including fault, performance, configuration, and security management
- Technologically, it is a set of Information Technology tools, which among others, incorporate the methods of Artificial Intelligence, Knowledge Management, Distributed Systems, and Object Orientation

Altusys Corporation

6

Event Correlation System



- The Event Correlation System includes two main processes:
- Real-Time Event Correlation Process
 - On-line Knowledge/Data Provisioning Process

Altusys Corporation

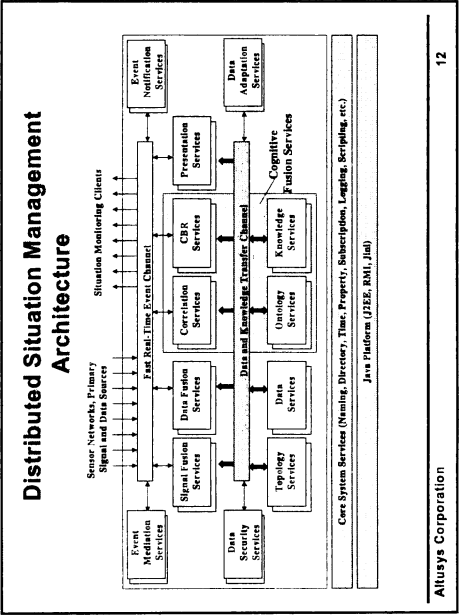
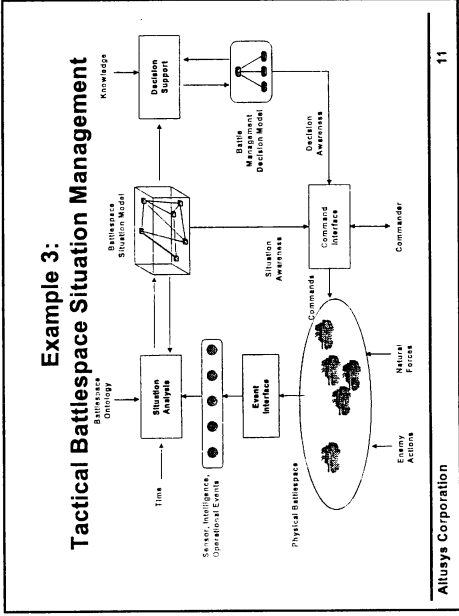
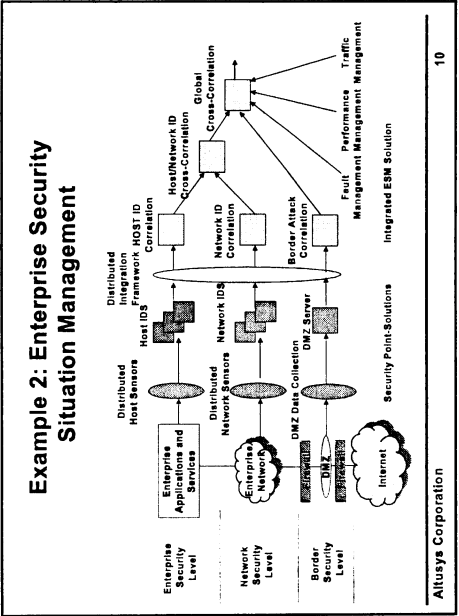
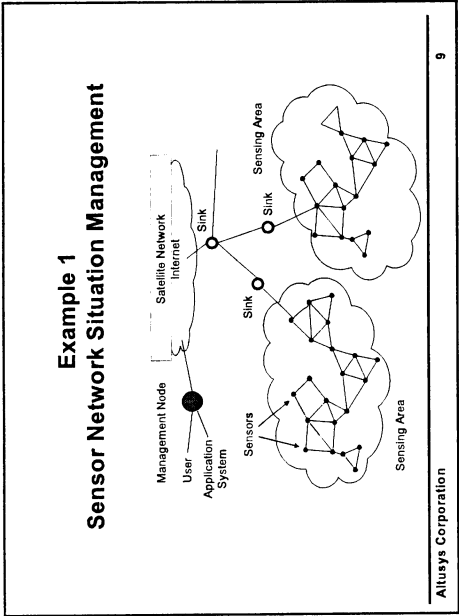
7

Event Correlation Classes

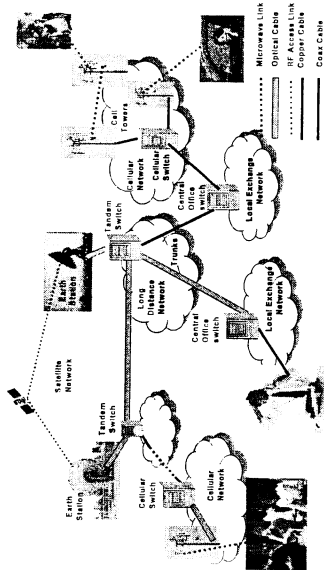
- | | |
|--|-------------------|
| 1. $[a, a, \dots, a] \rightarrow [a]$ | Compression |
| 2. $[a, p(a) < H] \rightarrow [\text{nil}]$ | Filtering |
| 3. $[a, C] \rightarrow [\text{nil}]$ | Suppression |
| 4. $[n \ x] \rightarrow b$ | Count |
| 5. $[n \ x, p(a)] \rightarrow a, p'(a), p' > p$ | Escalation |
| 6. $[a; a \text{ subclass } b] \rightarrow b$ | Generalization |
| 7. $[a; b \text{ subclass } a] \rightarrow b$ | Specialization |
| 8. $[a \ T \ b] \rightarrow c$ | Temporality |
| 9. $[a, b, \dots, T, \text{AND, OR, NOT}] \rightarrow c$ | Logic/Temporality |

Altusys Corporation

8



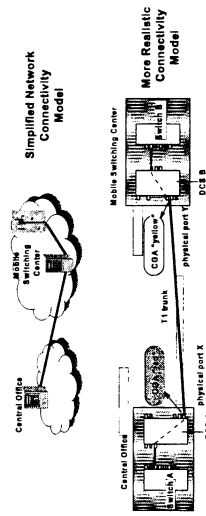
Case Study: Situation Management in Telecommunication Networks



Altusys Corporation

13

T1 Trunk Fault Diagnostics Based on Situation Analysis



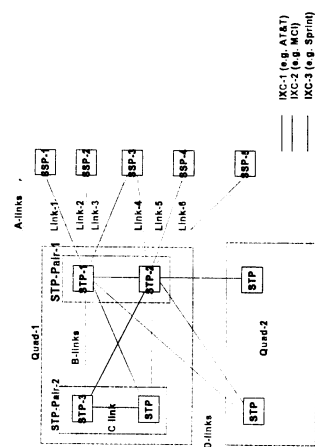
Situation Recognition Rule

IF there is a CGA Red Alarm from the physical port X belonging to the DCS A
AND there is a CGA Yellow Alarm from the physical port Y belonging to the DCS B
AND the ports X and Y are connected by a T1 trunk
AND the alarms CGA RED and CGA Yellow are coming within 3 seconds
THEN there is facility disconnect between switches A and B

Altusys Corporation

14

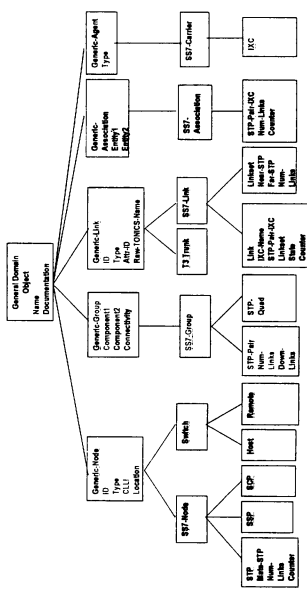
SS7 Network Situation Management



Altusys Corporation

15

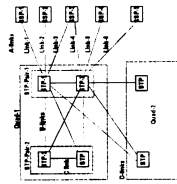
Ontology-Based Network Topology Modeling



Altusys Corporation

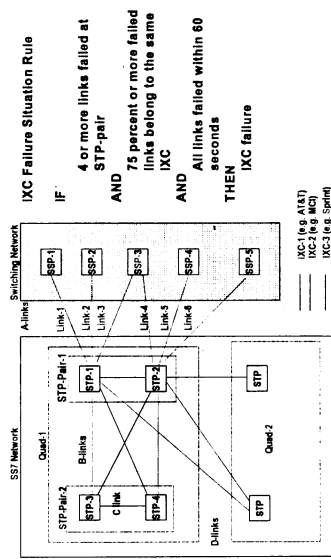
16

Topology Model



17

SS7 Network Link Failure Situation Recognition



18

Management

- Entities are things that makes sense to talk within a concrete problem solving context, e.g. battle tank is entity, router is entity, and broadband IP service is entity
- Topology of a system is an organized collection of component entities, where the organization is built up via multiple structural containment, connectivity, class, administrative, and other domain-specific relations, e.g.
 - Routing table IS-PART-OF Router
 - TankUnit SUBORDINATED-TO FormationA
 - ClassFaaSService IMPLEMENTED-BY CircuitXYZ
- Examples: battlefield topology, network topology (network configuration), service topology
- Entities could be active ones, i.e. the ones, which change their parameters over time, or passive ones, whose parameter values are considered constant during the observed time period
- Entities may have a lifecycle: they appear, change and disappear

19

Future Research Directions

- **Ontology-based situation management**
- **Situation specification languages and tools**
- **Self-organizing and autonomic systems using situation management**
- **Situation Transition Graphs (STG)**
- **Integration of lower-level (signal and data level) situation management with the higher level situation management**
- **Synergy between cognitive information fusion and situation management**
- **Predictive modelling for situation/threat analysis**
- **Situation learning**

20