

A faint, light gray world map is visible in the background of the slide, centered behind the text.

Looking at Code With Your Safety Goggles On

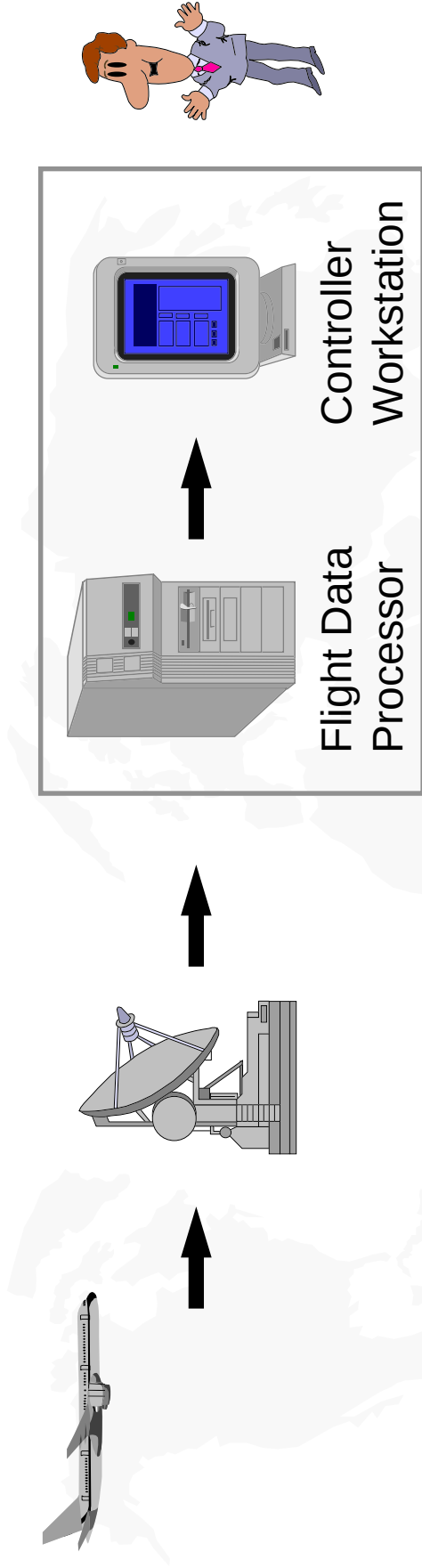
Ken Wong

Department of Computer Science
University of British Columbia

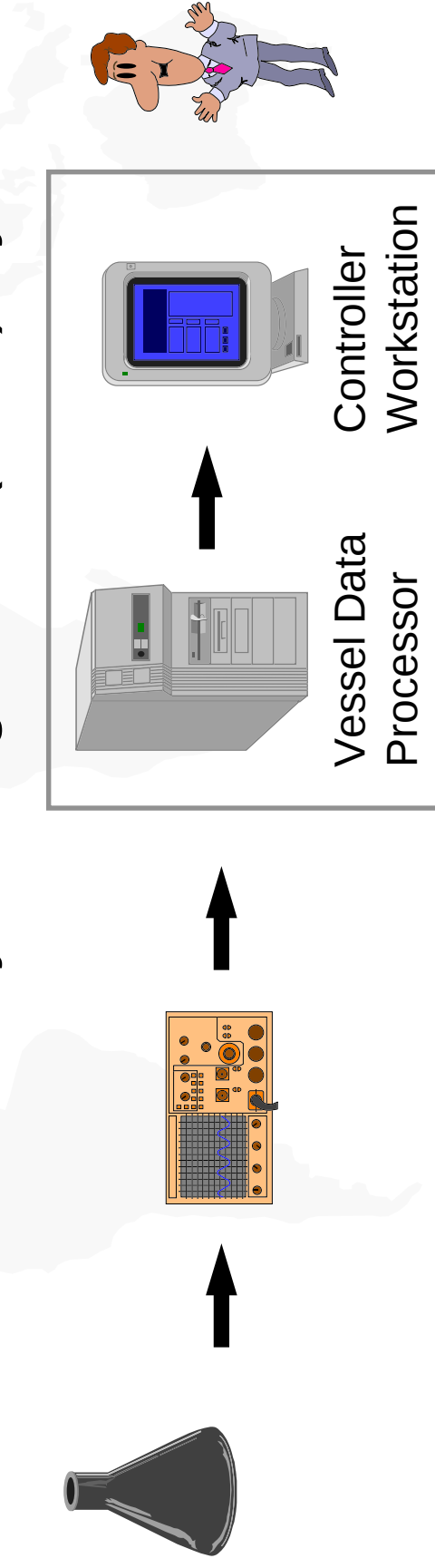
Air Traffic Management (ATM)

- ◆ Raytheon Systems Canada Ltd.
- ◆ Real-time information system
- ◆ Large scale Ada system
 - 700,000 production SLOC + COTS
- ◆ Modern architecture
 - Object-oriented, layered, distributed

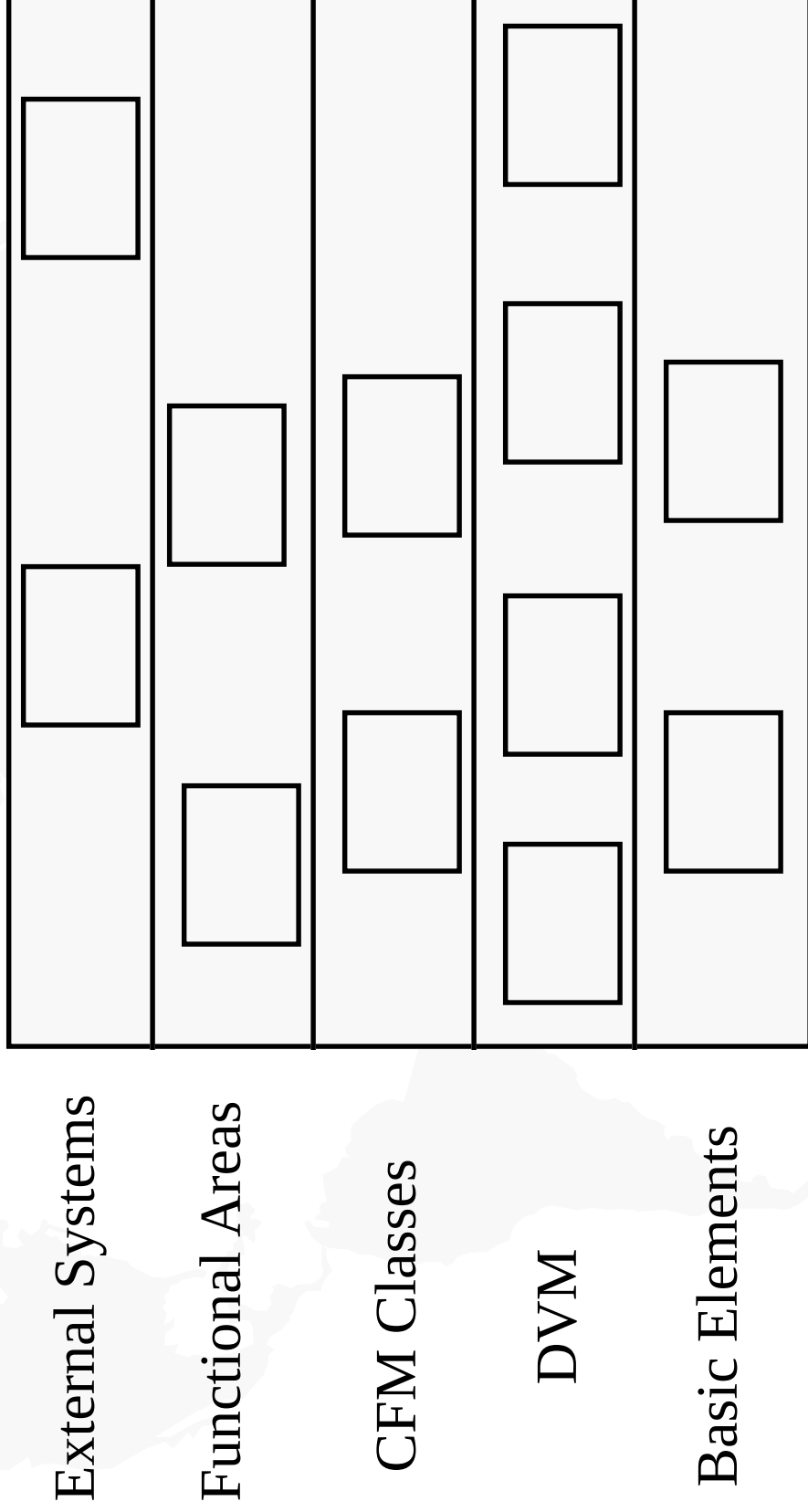
Air Traffic Management (ATM) System



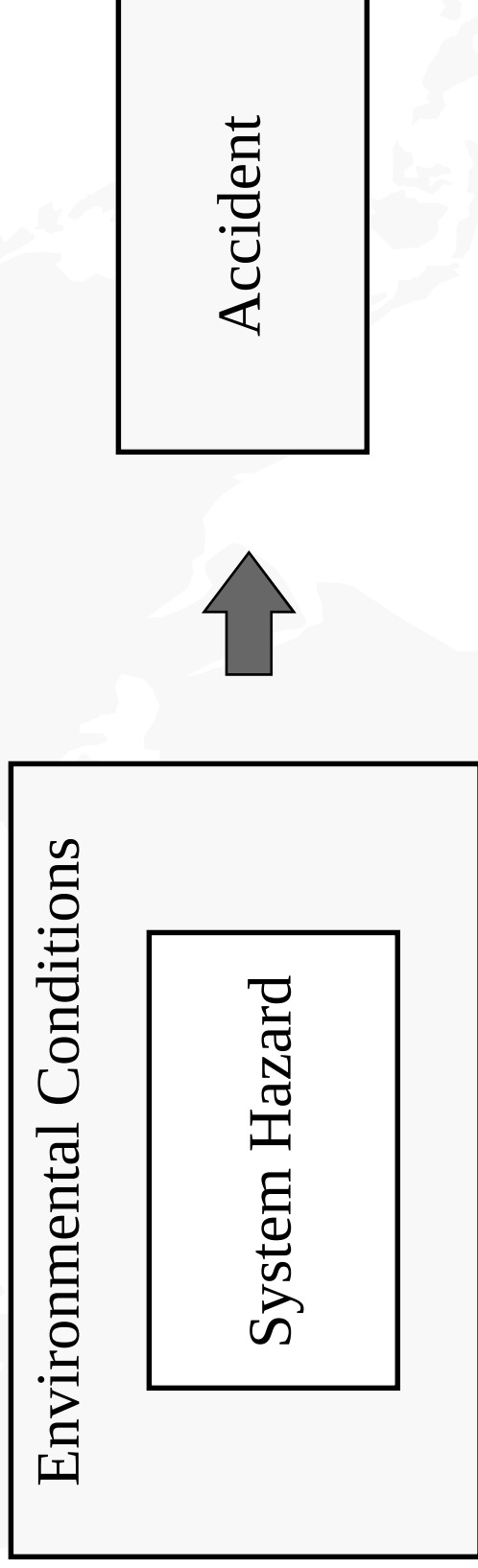
Chemical Factory Management (CFM) System



Static Architecture



System Safety Engineering



- ◆ Identification, analysis, elimination or control of system hazards

CFM Safety

- ◆ **Accidents**
 - e.g., Vessel rupture, fire or explosion
- ◆ **System Hazards**
 - e.g., An “invalid” temperature, D , is displayed for vessel V at time T
- ◆ **Hazard Analysis**
 - e.g., temperature value is stale or corrupted

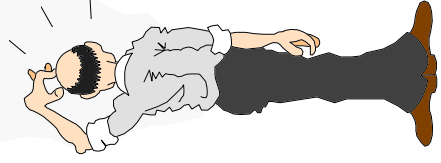
Safety Verification

System
Hazard

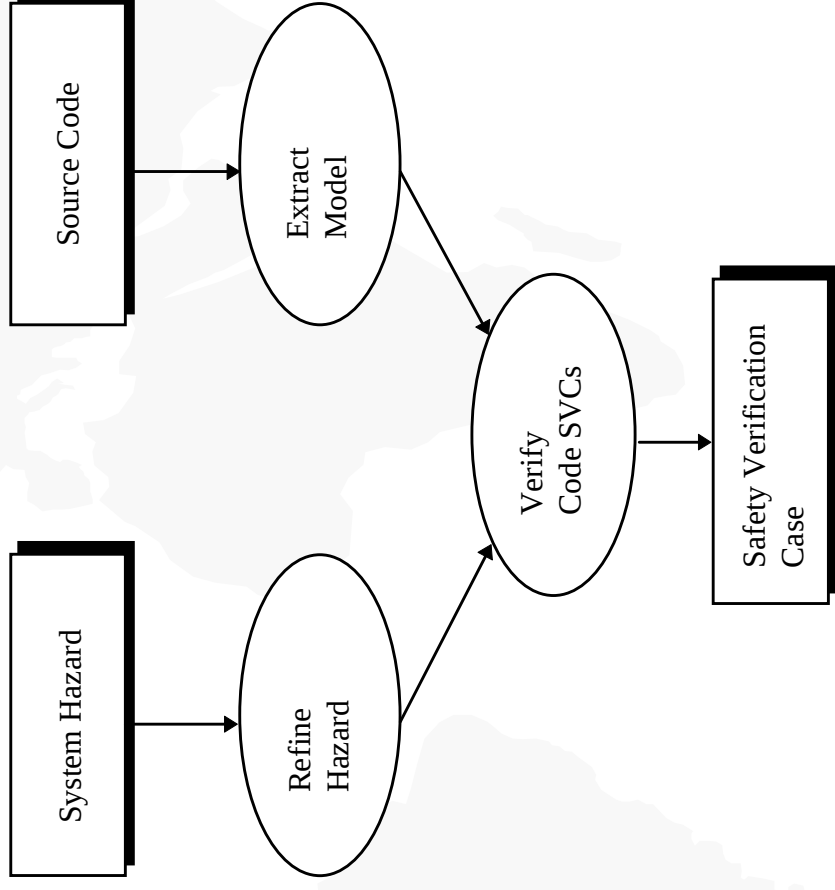


Source
Code

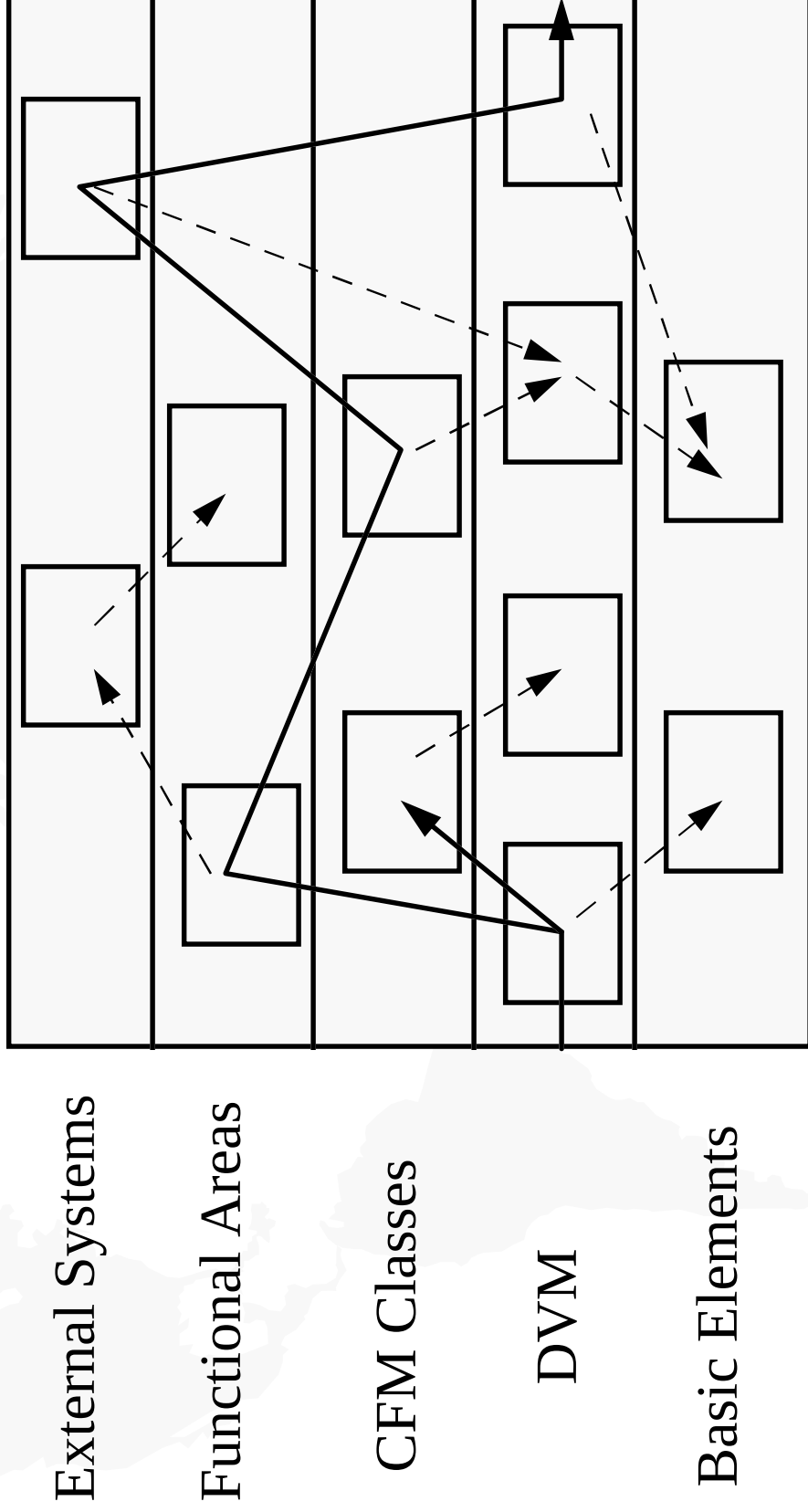
?



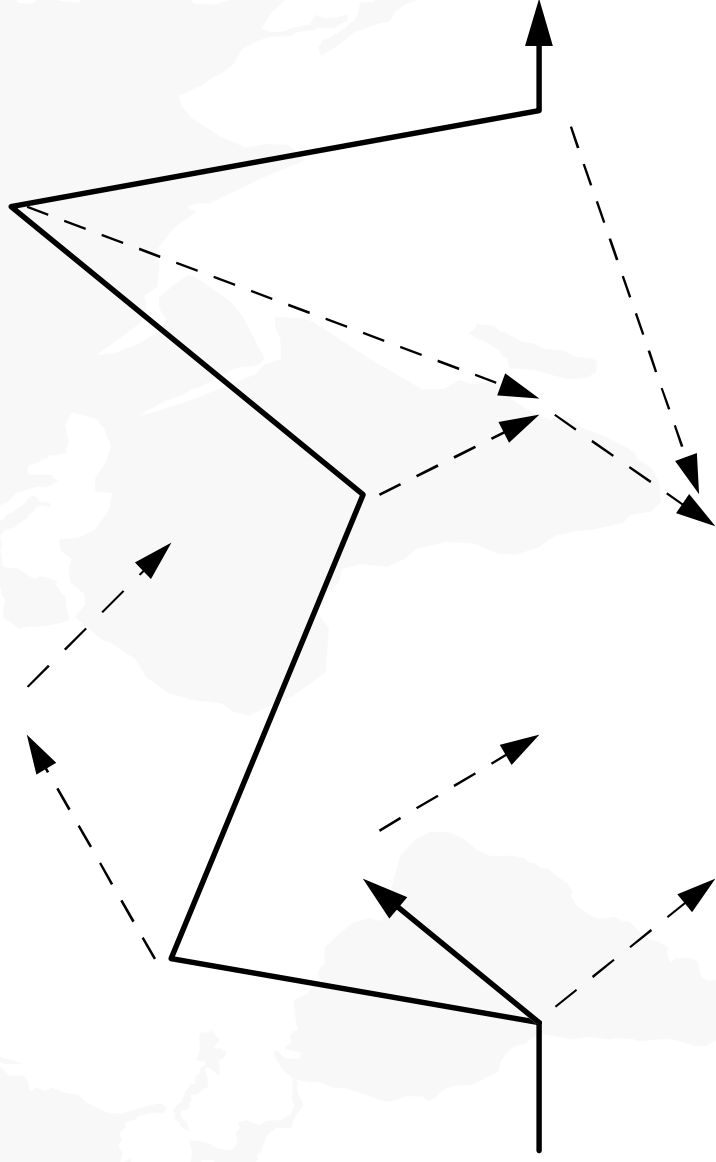
Safety Verification Case



“Long Thin Slice” Problem



Code Model Extraction



Code Model

- ◆ Properties
 - Conservative, complete, tractable
- ◆ Representation
 - Textual description
 - Executable - e.g., “SPARK”ify

Bottom-Up Extraction

- ◆ Search code
 - Forward or backward
- ◆ Record Search
 - Textual, acyclic graph
- ◆ Tools
 - Software development environment - e.g. Apex
 - Static analysis - e.g., Ada Analyzer, McCabe
 - Roll your own - e.g., ASIS

Top-Down Extraction

A faint, light gray world map is visible in the background of the slide, centered behind the text.

- ◆ Transform code
 - Fillet, Flatten, Filter, Partition, Translate
- ◆ Record transformations
 - Textual, executable script

References

- ◆ <http://www.cs.ubc.ca/formalWARE/safety.htm>
- ◆ Ensuring the Inspectability, Maintainability and Repeatability of the Safety Verification of a Critical System, UBC Technical Report 98-06.
- ◆ Bruce Elliott and Jim Ronback, “A System Engineering Process For Software-Intensive Real-Time Information Systems”, in Proceedings of the 14th International System Safety Conference, Albuquerque, New Mexico, August 1996.
- ◆ Philippe B. Kruchten and Christopher J. Thompson, “An Object-Oriented, Distributed Architecture for Large Scale Ada Systems, in Proceedings of the TRI-Ada ‘94 Conference, Baltimore, November 6-11, 1994, ACM.