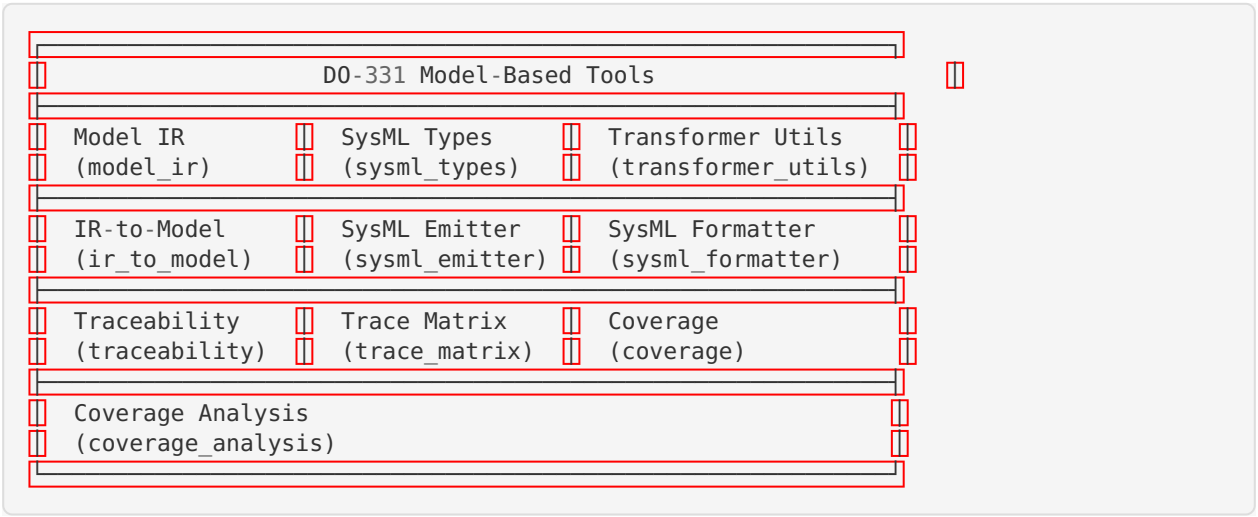
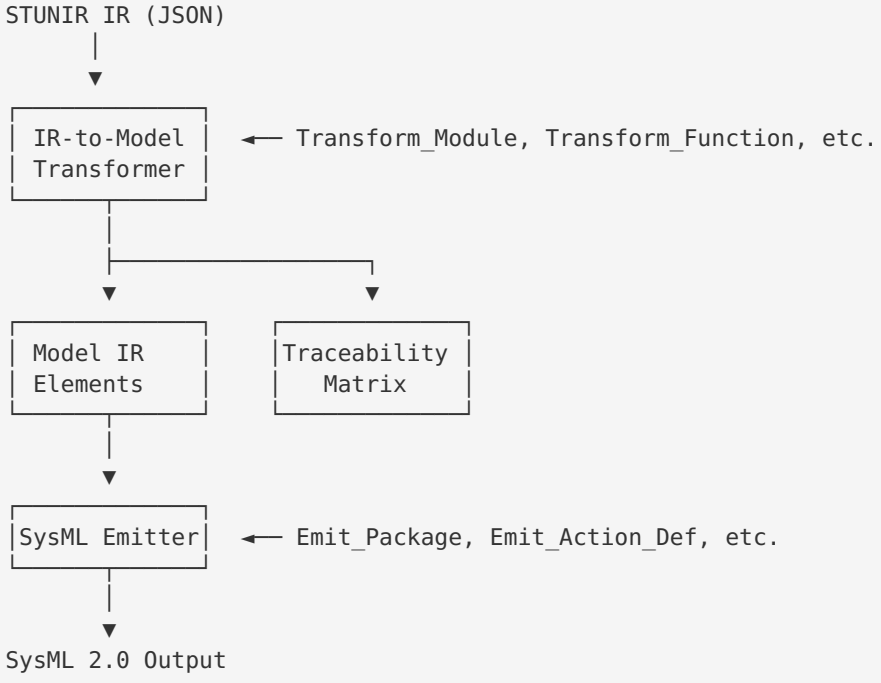
DO-331 Tools Architecture

Component Overview



Data Flow



Key Design Decisions

1. Ada SPARK Implementation

All components are implemented in Ada SPARK with:
- `SPARK_Mode => On` for formal verification
- Bounded types (no dynamic allocation)

- Pre/Post contracts where appropriate
- No runtime exceptions

2. Bounded Data Structures

```
Max_Elements       : constant := 10_000;
Max_Name_Length    : constant := 256;
Max_Trace_Entries  : constant := 50_000;
Max_Coverage_Points: constant := 100_000;
```

3. Type Safety

- `Element_ID` for unique identification
- `Element_Kind` enumeration for type discrimination
- `DAL_Level` for compliance level
- `Coverage_Type` for coverage point classification

4. Transformation Rules

IR Element	Model Element	DO-331 Objective
module	package	MB.2
function	action def	MB.3
type	attribute def	MB.2
if/else	decision	MB.3
state	state	MB.3
transition	transition	MB.3

File Organization

```
tools/do331/
├── src/           # Ada SPARK source
├── tests/         # Test programs
├── docs/          # Documentation
├── examples/      # Example files
├── bin/           # Built binaries
├── obj/           # Object files
├── proof/         # SPARK proof artifacts
├── do331.gpr      # GNAT project file
└── Makefile       # Build automation
```