How Does One Design For Verifiability?

There follows a high level process flow for designing software systems to be verifiable.

1. Begin with a thorough English narrative specification of the problem.
2. Do a domain analysis which:
    a. Specifies a set of components from which the system can be constructed
    b. Specifies a set of attributes in which the components can be described
    c. Specifies the relationships among the components
3. Map the domain analysis onto a software architecture specification in a formal representation. The representation must include specification of components, properties of components and relationships among components.
4. Specify the external behavior of the system as a set of properties.
5. Project those properties onto the properties of the components through the relationships between the components.
6. Verify the properties on the components
7. Compose the verified components using the properties which have been verified on the components