**Question 4**

i) Sketch out the structure of a suitable safety argument for this software, making best use of the evidence identified in points 1-12 above. Ideally, this argument structure should be presented in GSN, although there will be no penalty if you are unfamiliar with GSN and choose to use another method provided that the argument is clear.

**Solution**: In order to present argument structure in Goal Structuring Notation, identify goals to be supported. In this question, its **goal** is *Coyote Software is acceptably safe within Tokushima Product*. In this goal, it could be solved by one **strategy**, which is *Argument over product and process of the calibration data*. In order to perform this approach, the two **sub goals**, which are *G2 Software does not raise hazard on Tokushima Product* and *G2 Software does not have hazard in itself*. For the Goal 2, the software performance situation should be assess. For the Goal 3, the software should be perform hazard analysis to make sure the software have no hazards. At the same time, this goal has four **contexts**, which are *Coyote Software*, *Tokushima Product*, *Safety Standard of Software* and *Software Running*, act as the states to Goal 1 and Goal 3. As the result, the **top** part of Goal Structuring Notation could be diagram as following:

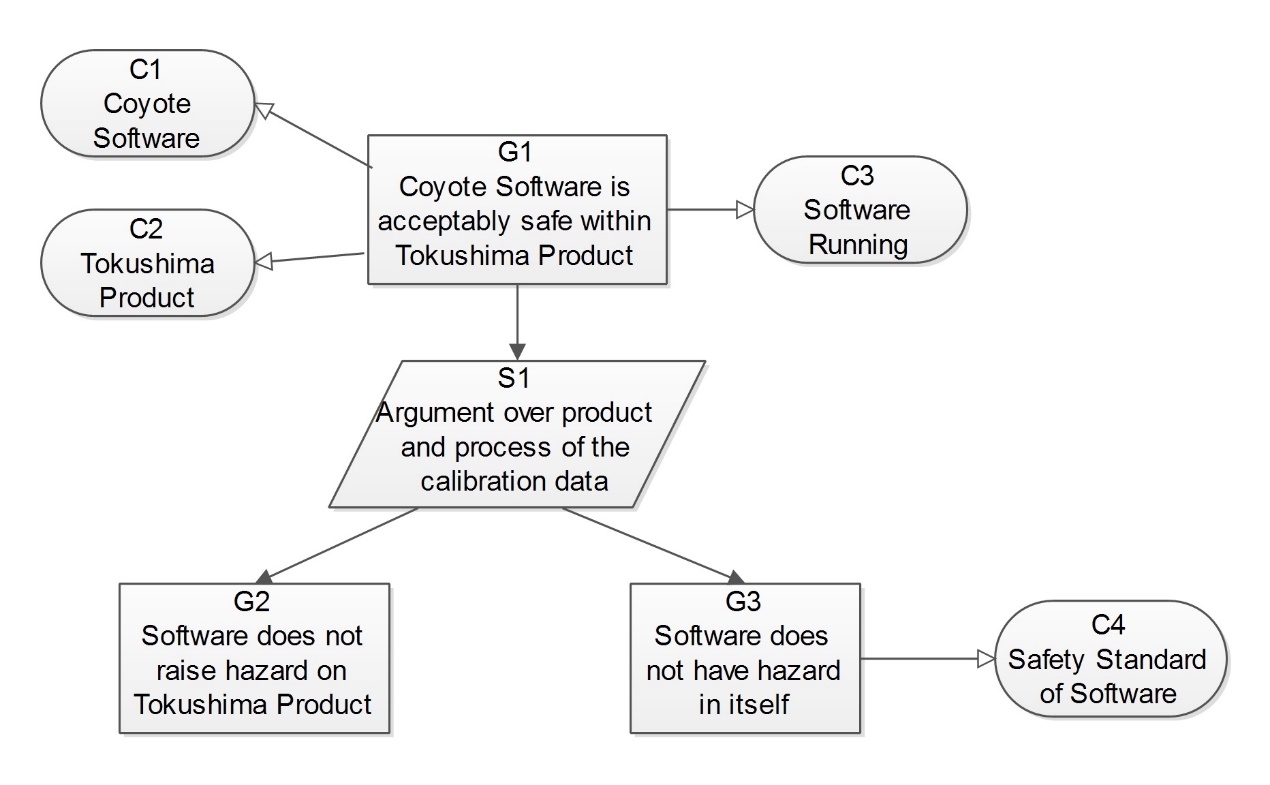


Figure :

According to the same approach to develop argument diagram, continue to define basis on goals states and strategy, than identify new goals until identify basic solution. The following two figures are the whole result of a goal structuring notation figure which represents to the argument structure (Some goals lock of evidence to support).

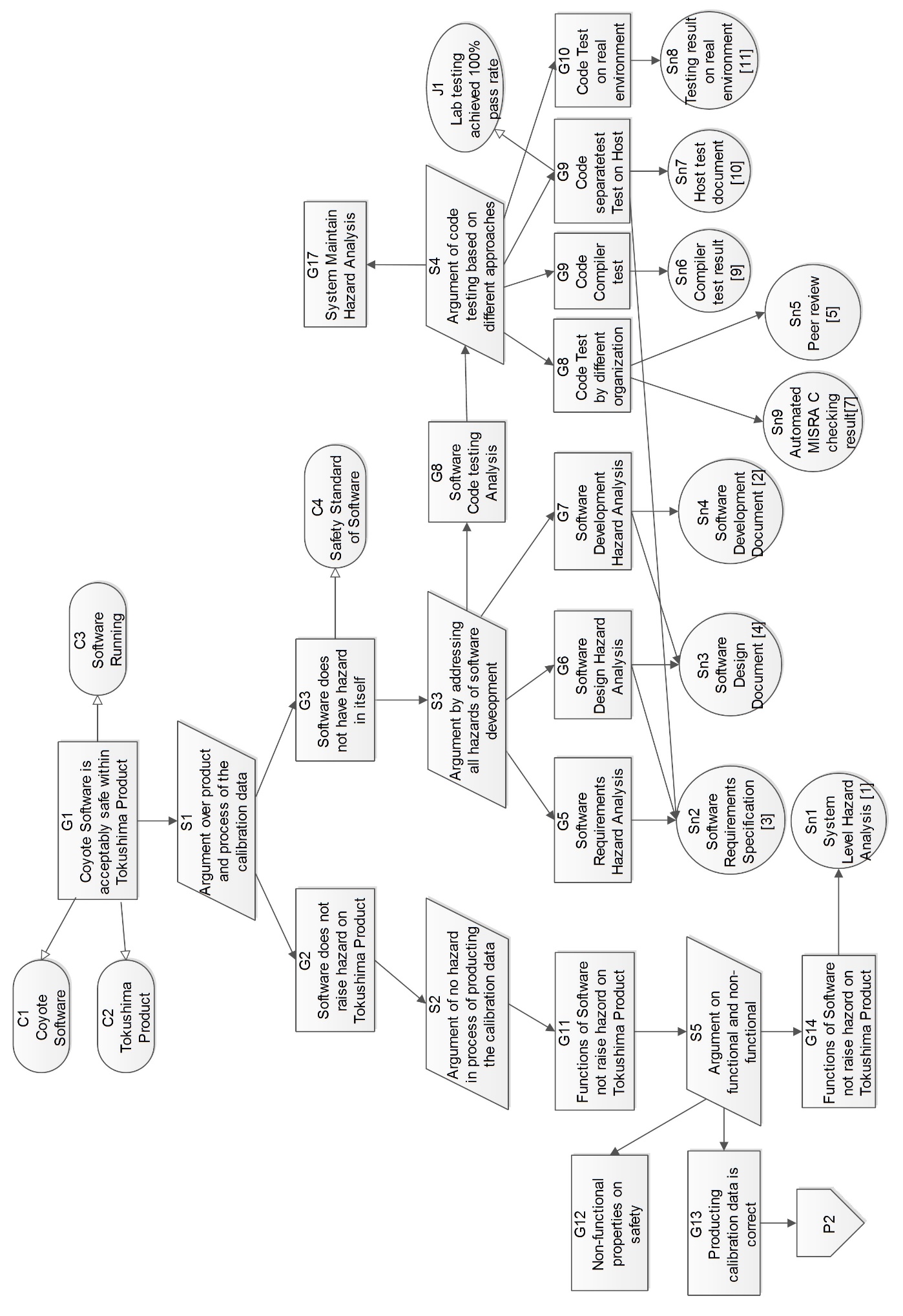


Figure:

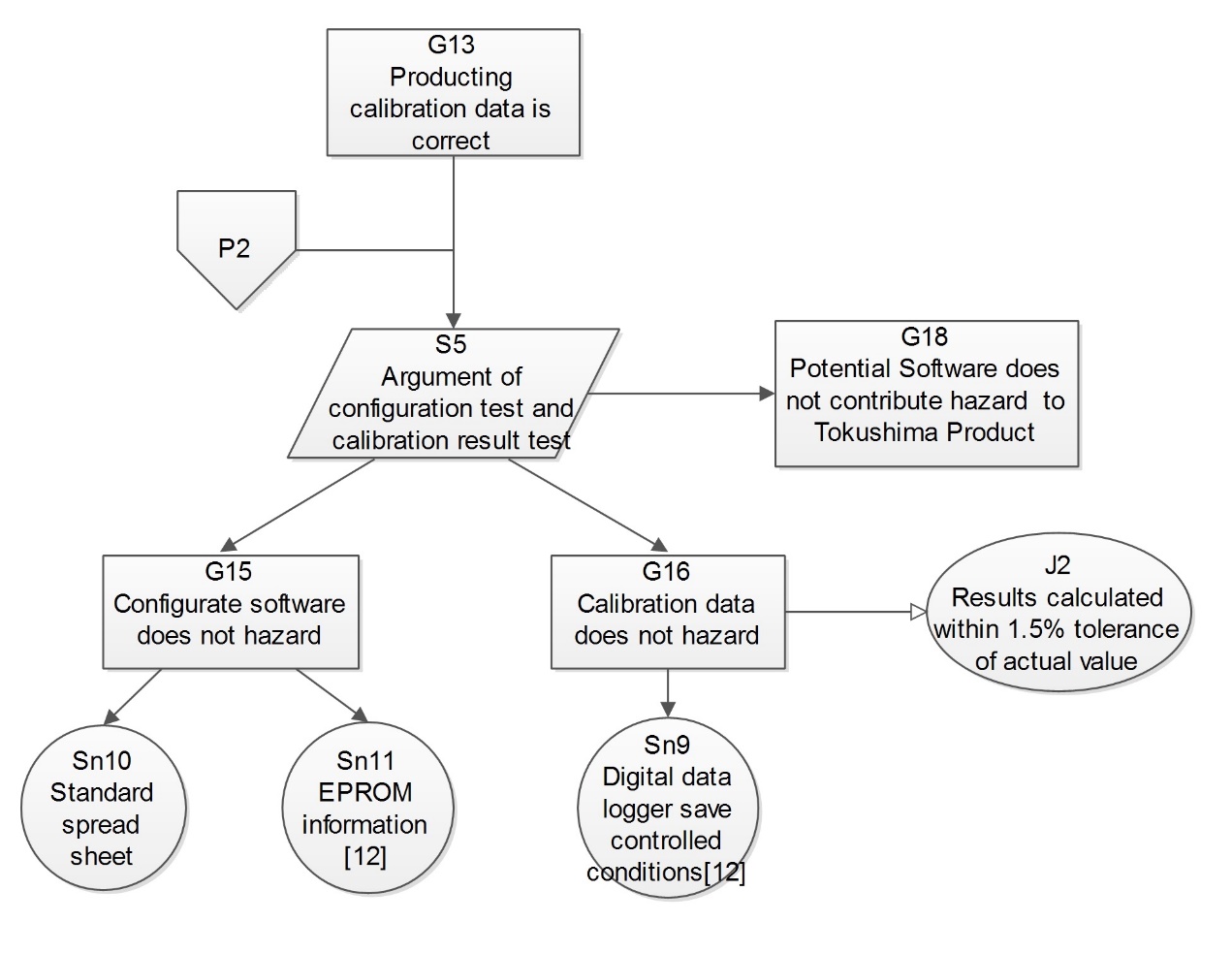


Figure:

The Figure and are the structure of a suitable safety argument for this software, which presented in GSN.

ii) Is there sufficient evidence available to make a compelling argument? If not, identify what else you believe is needed, and explain why. Is any of the evidence identified in points 1-12 above of no use in supporting your argument?

**Solution**: In this argument, the **evidence** is **not sufficient** because there are some part of sub-goal **lock of** evidence to support. This situation could be easy to find from the **figure** and **figure**. For *Goal 12- Non-functional properties on safety*, the Coyote Company did not provide evidence to analysis the non-functional hazard. For the *Goal 17- System Maintain Hazard Analysis*, the Coyote Company did not provide evidence to analysis the hazards in their product maintain process. Moreover, the *Goal 18 – Potential Software does not contribute hazard to Tokushima Product*, the Coyote Company did not provide the system level hazard identification and risk analysis to the in the compatibility between software from Coyote and crane from Tokushima. At the same time, several evidence have the **defect** on **completeness** or **effectiveness** of document, and effect on the argument. For the *Sn4 – Software Development Document*, did not follow the form style like safety integrity level or Development Assurance Level, which are only record brief from the team members. This kind of evidence could not be used to demonstrate the development process.

As the result, the Coyote Company should provide the evidence relative to s*ystem non-functional hazard analysis to support* to support *Non-functional properties on safety*, *system maintain hazard analysis* to support *System Maintain Hazard Analysis*, *system level hazard identification and risk analysis based on Coyote functio*n to support *Potential Software does not contribute hazard to Tokushima Product*. These evidences would use to support argument, and make it compelling. At the same time, Coyote Company should provide the **formal documents** which in standard software project development management style on **development** **process** of software to act as the evidence to support *Software Development Analysis*.

There are several evidences does not used to support to my argument. There are the **comments** in the codes which could trace back to Software Requirement Specification. The **code** which **subjected** to automated MISRA C conformance checking, which is useless, unless get the feedback report from official organization.