You have 90 minutes to work on this exam. It is a "closed-book/closed-notes" test.

IMPORTANT: Students who have already taken UF course CEN 4072/6070, Software Testing and Verification, should work PROBLEMS 1-11 AND 19-23 ONLY. All other students should work PROBLEMS 1-18 ONLY. NO CREDIT WILL BE GIVEN for working additional problems.

You should assume that all variables represent INTEGERS, unless otherwise indicated.

PRINT your name above NOW and sign the pledge at the bottom of the last page, if appropriate, when you are finished.

You will be given a blank piece of "scratch paper," but all answers must be written on the exam itself.

PLEASE PRINT ANSWERS IN THE SPACE PROVIDED ONLY – PREFERABLY USING A BALL-POINT PEN TO INCREASE LEGIBILITY. Good luck!

1. (8 pts.) Sommerville notes that while "traditional" engineering disciplines have had no difficulty in incorporating mathematical analysis into their processes, software engineering has not followed the same path. Despite the predictions of many software engineering researchers in the 1980s, so-called formal methods of software development are not widely used in industrial software development today. Sommerville argues that there are four main reasons for this. Two of these are the limited scope of formal methods, and the limited scalability of formal methods. Briefly describe the other two reasons he gives. (Please print – do not write cursively. Your writing must be legible in order to receive credit.)
2. (14 pts.) Match each description below to the **SINGLE MOST APPROPRIATE TERM** among the following. (Note: terms may apply to none, one, or more than one description.)

A. predicate  
B. universal quantifiers  
C. constructor operations  
D. operational specification  
E. axioms  
F. pre-condition  
G. model-based specification  
H. post-condition  
J. assignment function  
L. inspection operations  
M. function-based specification  
N. existential quantifiers  
O. operation signatures  
P. algebraic specification  
R. Z  
S. schema signature

___ Defines the entities that make up the state of the system being specified using Z.

___ A specification approach that defines required program behavior in terms of **intended program functions**.

___ Used to specify program data mappings; its domain corresponds to the initial data states that would be transformed into final data states by a suitable program.

___ That part of a schema which defines conditions that are always true.

___ Used to assert that some predicate holds FOR AT LEAST ONE or FOR SOME member of a given set.

___ A specification approach whereby a system is specified in terms of a **state model** and operations are defined in terms of changes to system state.

___ Expresses constraints on program variables that an implementer may assume will hold **before** program execution.

___ A specification approach well suited for specifying the interfaces of objects and abstract data types.

___ This specification approach can become cumbersome when object operations are not independent of object state.

___ Expresses obligatory conditions / relationships among program variables **after** execution in model-based specification.

___ A mature **notation** for model-based specification that uses sets and relations between sets.

___ Defines the **semantics** of operations defined over a sort in an algebraic specification.

___ Defines the interface **syntax** of an object class or abstract data type.

___ A specification approach whereby a system is specified in terms of its operations and their relationships via axioms.
3. (12 pts.) Match each application or description below to the **SINGLE MOST APPROPRIATE** type of architecture among the following. (Note: architecture types may apply to none, one, or more than one application or description.)

A. two-tier client/server (C/S) architecture with thin clients  
B. two-tier client/server (C/S) architecture with fat clients  
C. multi-tier client/server (C/S) architecture  
D. distributed component architecture  
E. peer-to-peer architecture (P2P)  
F. software as a service (SaaS)  
G. service-oriented architecture (SOA)  
H. master-slave architecture

___ Sommerville illustrates this architecture with a scalable Internet banking system.

___ An approach to structuring a software system as a set of separate, stateless services that may entail multiple providers and may be distributed.

___ Commonly used in real-time systems where there may be separate processors associated with data acquisition from the system’s environment, data processing, and computation and actuator management.

___ Well known examples include web-based mail systems such as Yahoo! and Gmail, and office application such as Google docs.

___ This architecture has the advantage of being highly redundant and therefore both fault-tolerant and tolerant of nodes disconnecting from the network.

___ An example of this type of architecture might be an easily extendable data mining system comprised of multiple standard data sources, a number of independent data “integrators” each attempting to deduce different relationships, graphical relationship “visualizers” and report generators.

___ Applications with relatively stable end-user functionality used in an environment with well-established system management.

___ Browsing the Web is the most common example of a situation where this architecture is used.

___ Sommerville illustrates this architecture with a real-time traffic control system that has three logical processes that run on separate processors.

___ An example of this type of architecture is a banking ATM system for which the hardware in the teller machine carries out most of the customer-related processing associated with transactions.

___ Provides functionality on a remote server with client access through a web browser. The server maintains the user’s data and state during an interaction session. Transactions are usually long (e.g., editing a document).

___ Some developers of systems based on this architecture have opted to replace existing “inefficient” protocols developed to be open standards with so-called RESTful protocols having inherently lower overhead.
4. (4 pts.) Sommerville notes that the 1990’s “Bootstrap project” (Haase, Kuvaja, et al.), which uses the SEI’s maturity levels, had the goal of addressing a particular shortcoming of the SEI process maturity model. What specific shortcoming did it attempt to address?

5. (10 pts.) Match each description below to the **SINGLE MOST APPROPRIATE AOSD RELATED TERM** among the following. (Note: terms may apply to none, one, or more than one description.)

<table>
<thead>
<tr>
<th>A. advice</th>
<th>I. tangling</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. scattering</td>
<td>J. join point model</td>
</tr>
<tr>
<td>C. knotting</td>
<td>K. guidance</td>
</tr>
<tr>
<td>D. aspect</td>
<td>L. pointcut</td>
</tr>
<tr>
<td>E. core concerns</td>
<td>M. cross-cutting concerns</td>
</tr>
<tr>
<td>F. braiding</td>
<td>N. feature</td>
</tr>
<tr>
<td>G. join point</td>
<td>O. weaving</td>
</tr>
<tr>
<td>H. knitting</td>
<td>P. scrambling</td>
</tr>
</tbody>
</table>

___ An event in an executing program where the code associated with an aspect may be executed

___ A statement, included in an aspect, that defines where code should be executed in a program

___ An abstraction designed to encapsulate functionality associated with a cross-cutting concern

___ Aspect code implementing a concern

___ Act of combining objects, methods, and aspects to create an executable program

___ Requirements such as those associated with quality of service issues that apply to a system as a whole rather than those associated with the primary functional services a system provides

___ Occurs when the implementation of a concern is dispersed across more than one component in a program

___ Occurs when a module in a system includes code that implements different system requirements

___ Functional requirements that directly relate to a system’s primary purpose

___ The set of events that may be referenced in a pointcut
6. (3 pts.) Sommerville notes that “Aspects are completely different from other program abstractions...”. Which one of the following best describes the distinguishing characteristic of aspects? (Circle ONE only.)

   a. The interaction between aspects and other program abstractions is strictly asynchronous.

   b. There is a clear separation between the definition of the abstraction and its use. (You cannot tell by examining an aspect where it will be called from.)

   c. Aspect transactions are typically “brief,” whereby a cross-cutting service is called, does something, and returns a result. With other abstractions, transactions are usually “long,” e.g., editing a document.

   d. Unlike other abstractions, an aspect itself includes a specification of where it should be executed.

   e. Aspects may only communicate with core components via middleware using remote

7. (8 pts.) In Chapter 22, Project Management, Sommerville discusses three related categories of risk: project risks, product risks, and business risks.

Fixed-price contracts, where the contractor bids a fixed price to develop a system, may be used to move project risk from the client to contractor. If anything goes wrong, the contractor must absorb cost overruns.

**Explain how the use of such contracts may increase the likelihood that some product risks will arise.**

(Please print – do not write cursively. Your writing must be legible in order to receive credit.)
8. (4 pts.) Sommerville describes Maslow’s human needs hierarchy as “being helpful up to a point” in explaining what motivates people, but feels there is a specific problem with it. Which one of the following describes this problem? (Circle ONE only.)

a. He feels that “the opportunity for self-actualization and establishing satisfying relationships in the workplace are perhaps the most important contributors to motivating team members.”

b. In large projects, team members spend a smaller proportion of their time in development activities (supported by development tools) and more time communicating (with one another) and understanding other parts of the system. Development tools, Sommerville argues, make no difference to this.

c. He feels Maslow does not adequately consider the importance of allowing people to fully experience what life has to offer outside the workplace. (Sommerville quips that “all work and no play does much more harm than simply making Jack a dull boy.”)

d. He feels that “praise from immediate managers, leadership attention (for example, one-on-one conversations), and a chance to lead projects or task forces” are even more effective motivators than meeting the needs identified by Maslow.

e. He feels that in addition to thinking about individual motivation, you also have to think about how a group as a whole can be motivated to achieve the organization’s goals.

f. (None of the above)

9. (4 pts.) What, according to Sommerville, “is likely to be the most cost-effective process improvement strategy” for small to medium-sized projects?

a. Adopting agile development practices.

b. Using the GQM approach.

c. Validating requirements to ensure that the resulting product will perform as intended in the user’s environment, using multiple techniques as appropriate.

d. Performing causal analysis of selected defects and other problems and proposing actions to address them.

e. Establishing and maintaining an organizational policy for planning and performing the project planning process.

f. Employing a process management and maturity-based approach.

g. Adopting plan-driven development practices.

h. (None of the above)
10. (10 pts.) Consider the following statements related to the CMMI process improvement framework. Circle either “true” or “false” as (most) appropriate. To compensate for random guessing, your score in points will be 2 times the number of [correct minus incorrect] answers, or 0 – whichever is greater. Therefore, if you are not more than 50% sure of your answer, consider skipping the problem.

a. The CMMI “Defined” level of maturity focuses on organizational standardization and deployment of processes. Each project has a managed process that is adapted to the project requirements. Process assets and process measurements must be collected and used for future process improvements.

b. CMMI assessments involve directly examining the processes employed during one randomly selected on-going project and rating these on a six-point scale.

c. “Institutionalization of good practice” requires introducing process control using statistical and other quantitative techniques, regardless of maturity level.

d. In contrast to the continuous model, the staged CMMI permits discretion and flexibility in improving specific process areas, while still allowing companies to work within the CMMI improvement framework.

e. The CMMI model identifies recommended practices within a process area that may be used, but these are not obligatory.

11. (3 pts.) As discussed in class, two common measures of software product reliability are “mean time to system failure” and “probability of no system failure in a specified time interval”. Based on Sommerville’s definition of process reliability, which one of the following would be the most appropriate measure of this process attribute? (Circle ONE only.)

a. Probability that the process can continue in spite of a process error

b. Mean development time to the discovery of a process error

c. Probability that a process error can be avoided or trapped before it results in a product error

d. Mean time required for the process to evolve in order to reflect changing organizational requirements or identified process improvements

e. Probability of no process error in a specified development time interval
12. (9 pts.) Using pre- and post-conditions, formally specify a program that would set variable LAST to the index of the last instance of the constant value K in the non-empty array A[1:N] if there is at least one occurrence of K in A, and to 0 otherwise.

13. (8 pts.) Using one or more concurrent assignment functions, provide a function-based specification for the program given below. X and Y are assumed to represent INTEGERS.

```
while X>0 do
    Y := Y+1;
    X := X-1
end_while
```

Hint: Your specification should reflect the function of the while-do statement as a whole, which can be easily deduced by observation.

14. (4 pts.) Which one of the following statements best captures the precise meaning of the weak correctness predicate, "{P} S {Q}\"? (Circle ONE only.)

a. P must hold before S executes and Q must hold if S terminates.

b. \{P\} S \{Q\} is \textit{true} unless Q could be false if S terminates.

c. If P holds before executing S, S must terminate in state Q.

d. If P holds before executing S, then Q will hold if S terminates.

e. \{P\} S \{Q\} is \textit{true} unless Q is always false when S terminates, given that P held before executing S.

f. \text{wp}(S,Q) = P
NOTE: if you have already taken CEN 4072/6070, Software Testing and Verification, DO NOT work problems 12-18! (Work problems 19-23 instead.)

15. (6 pts.) Consider each of the following assertions and circle either “true” or “false” as appropriate. (Note: “|x|” refers to the absolute value of variable x, and “<>” means “NOT EQUAL TO.”) To compensate for random guessing, your score in points will be 2 times the number of [correct minus incorrect] answers, or 0 – whichever is greater. Therefore, if you are not more than 50% sure of your answer, consider skipping the problem.

a. \{y=ax+b\} y := y+x \{y=(a-1)x+b\} true false
b. \{true\} while x <> 5 do x := x+17 \{|x|=5\} true false
c. \{x\geq0\} S \{x\geq0\} \Rightarrow \{x=17\} S \{x=17\} true false

16. (4 pts.) Recall the while-do loop Rule of Inference (ROI) that was given in class:

\[
\begin{align*}
P \Rightarrow I, & \quad \{I \land b\} S \{I\}, \quad (I \land \neg b) \Rightarrow Q \\
\{P\} \text{ while } b \text{ do } S \{Q\}
\end{align*}
\]

Consider a repeat-until loop with pre-condition P and post-condition Q, with semantics defined by the following control-flow graph:

```
{P}    \\
\downarrow    \\
S    \\
\downarrow    \\
\diamond b    \\
|    \\
F    \\
\downarrow    \\
{Q}    \\
|    \\
T    \\
\downarrow    \\
S    \\
```

Complete the Rule of Inference below for the repeat-until loop based on the same approach taken in class to derive the while-loop ROI:

\[
\begin{align*}
\{P\} S \{I\}, \\
\{P\} \text{ repeat } S \text{ until } b \{Q\}
\end{align*}
\]

------------------------------------------- please do not write below this line -------------------------------------------
17. (12 pts.) Prove the following assertion by using the while-do Rule of Inference with
the given invariant, I. All variables are assumed to represent INTEGERS.

\{x \geq 0\} \quad \text{Use I: } d = y - k

\begin{align*}
d &:= y \\
k &:= 0 \\
\text{while } k \leq x \text{ do} \\
&\quad d := d - 1 \\
&\quad k := k + 1 \\
\text{end_while}
\end{align*}

\{d = y - x\}
18. (9 pts.) Consider the assertion:

\{x=8\}

if (x<0) then
  x := x+10
end_if

\{x=8\}

Use the WEAKEST PRECONDITION-BASED METHOD to prove the assertion. **Show all steps.** (Note: your solution must clearly demonstrate your knowledge/understanding of the WEAKEST PRECONDITION-BASED METHOD.)
19. (4 pts.) Sommerville notes that the term (system) “dependability” was proposed by Laprie to reflect four related system attributes: safety, availability, security, and reliability. In addition to these main attributes, he identifies four other system dependability properties. One of these is “repairability”. List two of the other three properties (and no others).

20. (4 pts.) Sommerville points out that in addition to the fact that increasing the dependability of a system can significantly increase its development costs, systems designers usually have to trade off system performance and dependability. Explain why this is so. Be specific.

21. Sommerville notes that system reliability and availability are closely related, but sometimes one is more important than the other.

a. (6 pts.) Give precise definitions of reliability and availability.

b. (7 pts.) What specific system does Sommerville use to illustrate his claim that one can sometimes be more important than the other? Which of the two attributes is more important for the system he describes and why?
NOTE: Work problems 19-23 ONLY if you have already taken CEN 4072/6070, Software Testing and Verification!

22. (15 pts.) Match each example or description below to the **SINGLE MOST APPROPRIATE** term among the following. (Note: terms may apply to none, one, or more than one example or description.)

A. vulnerability  
B. system fault  
C. exposure  
D. human error  
E. hazard  
F. system failure  
G. asset  
J. risk  
K. threat  
M. system error  
R. accident  
S. control  
T. damage  
X. attack

___ Example (from the wilderness weather station): a programmer deciding that the way to compute the time for the next transmission is to add 1 hour to the current time (which works except when the transmission time is between 23.00 and midnight)

___ Measure of the probability that a system will cause an accident

___ Example: a password checking system that disallows user passwords that are proper names or words that are normally included in a dictionary

___ Weakness in a computer-based system that may be exploited to cause loss or harm

___ Example (from the wilderness weather station): no weather data is transmitted because the transmission time is invalid

___ An erroneous system state that can lead to system behavior that is unexpected by system users

___ Example: a weak password system which makes it easy for users to set guessable passwords

___ A condition with the potential for causing or contributing to an accident

___ Example: an unauthorized user will gain access to the system by guessing the credentials (login name and password) of an authorized user

___ A protective measure that reduces a system’s vulnerability

___ An unplanned event or sequence of events which results in human death/injury, damage to property, or to the environment

___ Example: someone actively impersonating an authorized user

___ A characteristic of a software system that can lead to a system error

___ Example (from the patient information system for mental health care): the records of each patient that is receiving or has received treatment

___ A measure of the loss resulting from a mishap
23. (16 pts.) Consider each of the following statements concerning static analysis and circle either “true” or “false” as appropriate. To compensate for random guessing, your score in points will be 2 times the number of [correct minus incorrect] answers, or 0 – whichever is greater. Therefore, if you are not more than 50% sure of your answer, consider skipping the problem.

a. Static analysis is not particularly useful for security checking because attackers tend to base their attacks on uncommon vulnerabilities. **true**  **false**

b. Static analysis techniques are system verification techniques that do not involve executing a program. **true**  **false**

c. Model checking uses specialized software tools to exhaustively check all feasible paths through the system being verified. **true**  **false**

d. When you test a program, defects can mask or hide other defects. **true**  **false**

e. Model checking is an example of alternative approaches to formally verifying programs using a deductive approach that are based on a less restrictive notion of correctness. **true**  **false**

f. Perhaps the most commonly used (non-automated) static analysis techniques are reviews and inspections, where a specification, design, program, etc., is checked by a group of people. **true**  **false**

g. Formal specification and proof of correctness can only guarantee that software will be reliable in *practical* use. **true**  **false**

h. Sommerville cites the failure of the Ariane 5 rocket in 1996 to show how a reluctance to use formal verification because of the associated expense can lead to accidents resulting in the loss of life. **true**  **false**