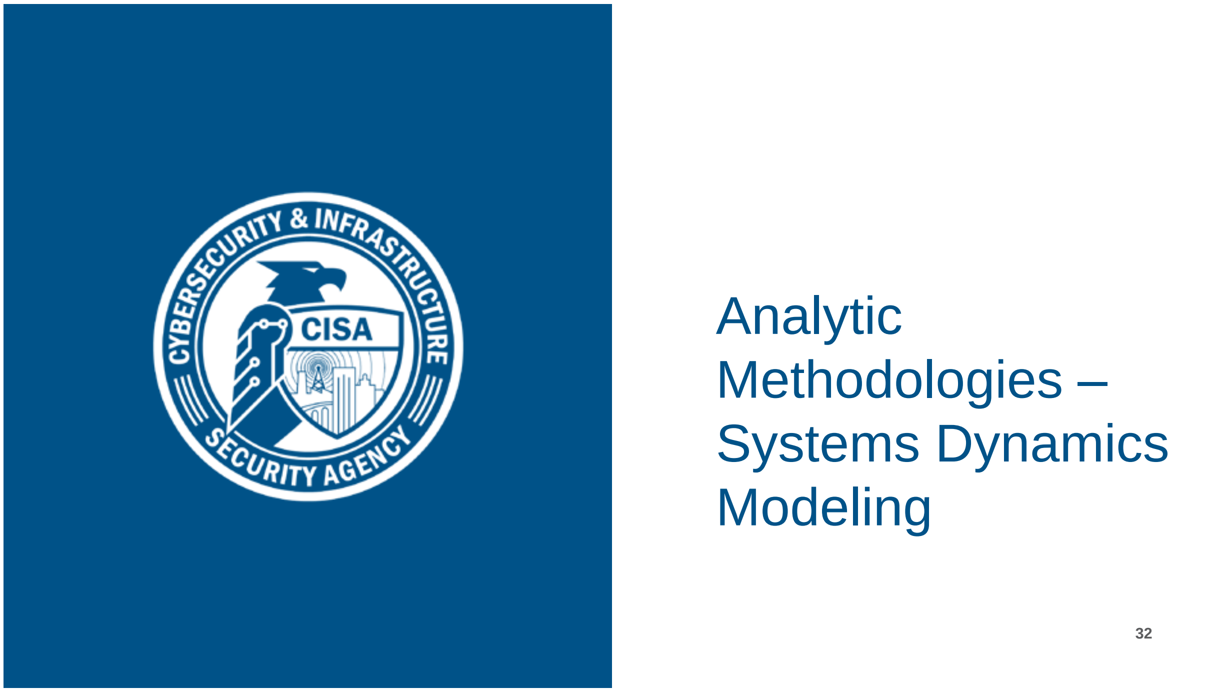
Analytical Methodologies – Systems Dynamics Modeling

Table of Contents

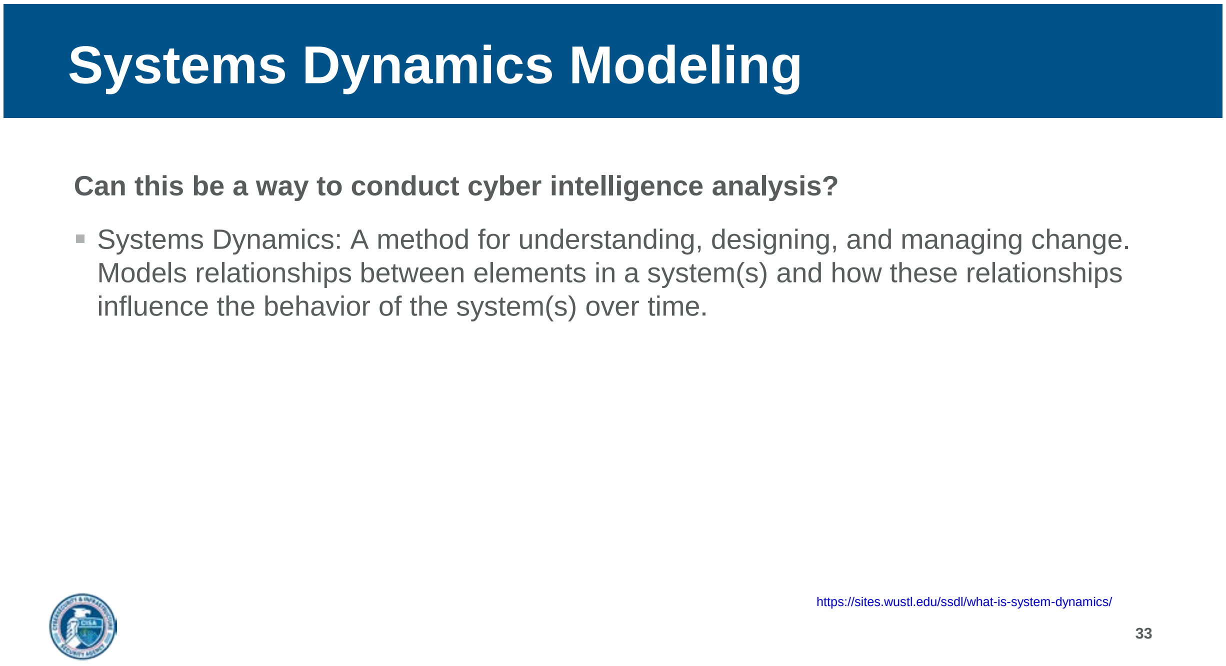
Analytic Methodologies – Systems Dynamics Modeling



Analytic Methodologies – Systems Dynamics Modeling

32

**032 Systems Dynamic Modeling is another type of methodology, and it's usually done to understand complex systems.



Systems Dynamics Modeling

Can this be a way to conduct cyber intelligence analysis?

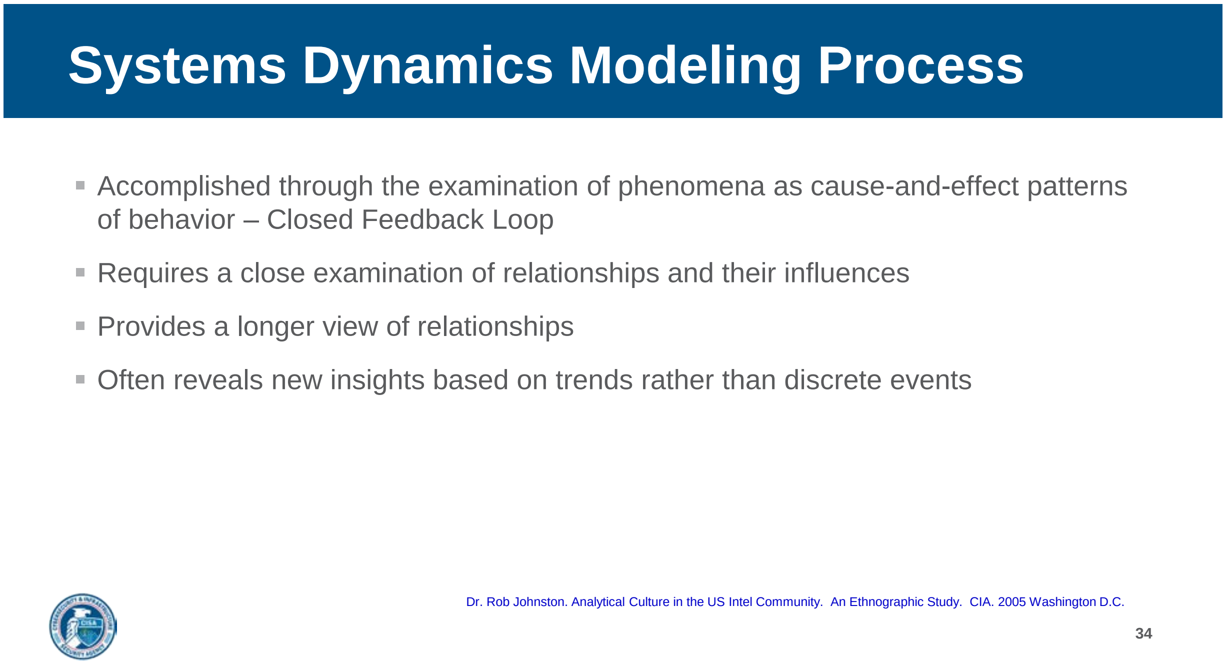
- Systems Dynamics: A method for understanding, designing, and managing change. Models relationships between elements in a system(s) and how these relationships influence the behavior of the system(s) over time.

https://sites.wustl.edu/ssdl/what-is-system-dynamics/

33

**033 More precisely, it is a method for understanding, designing and managing change, and it models relationships between elements in a system and how these relationships influence the behavior of a system over time.

Systems Dynamics Modeling Process



Systems Dynamics Modeling Process

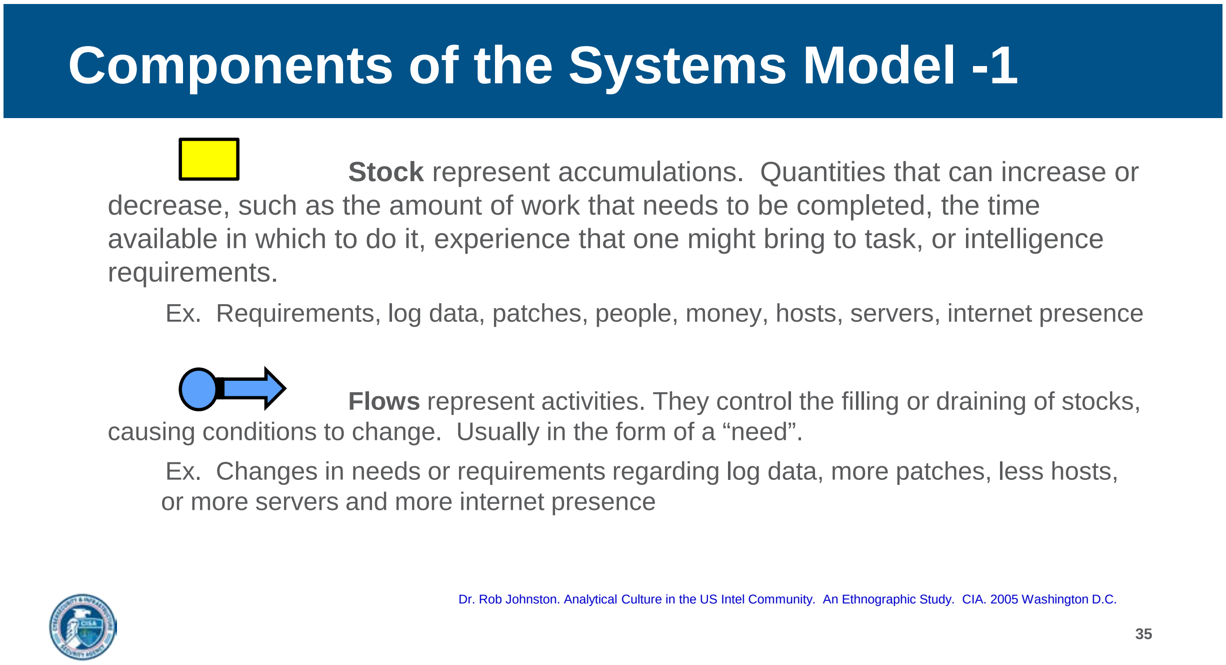
- Accomplished through the examination of phenomena as cause-and-effect patterns of behavior – Closed Feedback Loop
- Requires a close examination of relationships and their influences
- Provides a longer view of relationships
- Often reveals new insights based on trends rather than discrete events

Dr. Rob Johnston. Analytical Culture in the US Intel Community. An Ethnographic Study. CIA. 2005 Washington D.C.

34

**034 Systems Dynamics Modeling is usually accomplished through the experimentation of some type of phenomenon as a cause-and-effect pattern of behavior or a closed feedback loop, and generally speaking it requires a close examination of relationships and their influences. It provides a longer view of relationships, and it often reveals new insights based on trends rather than discrete, specific events. So let's take a closer look at Systems Dynamic Modeling and how it works.

Components of the Systems Model -1



Components of the Systems Model -1

Stock represent accumulations. Quantities that can increase or decrease, such as the amount of work that needs to be completed, the time available in which to do it, experience that one might bring to task, or intelligence requirements.

Ex. Requirements, log data, patches, people, money, hosts, servers, internet presence

Flows represent activities. They control the filling or draining of stocks, causing conditions to change. Usually in the form of a "need".

Ex. Changes in needs or requirements regarding log data, more patches, less hosts, or more servers and more internet presence

Dr. Rob Johnston. Analytical Culture in the US Intel Community. An Ethnographic Study. CIA. 2005 Washington D.C.

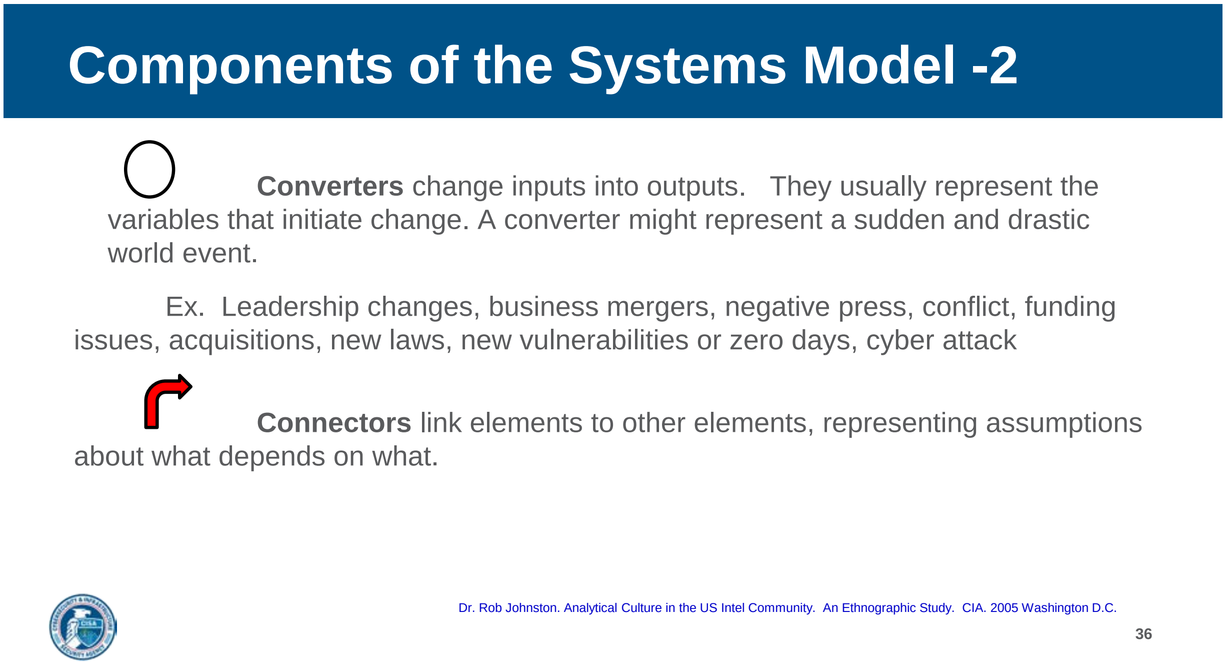
35

**035 This slide outlines the components of a systems model. You have these things called stocks. Stocks represent accumulations-- in other words, quantities that can increase or decrease, such as work that needs to be completed or the time available in which to do it, experience that one might bring to a task, or intelligence requirements even. So for example, maybe you have a requirement for more information about a particular threat, or no longer need a requirement. It can be log data or maybe a stock is to patch your systems on a network. If you need to be fully patched, the time it takes to get fully patched any time a new vulnerability comes out.

So flows represent activities. They control the filling or draining of stocks, causing conditions to change.

So a flow is usually some type of activity or some type of need that causes the filling or draining of stocks. So for example, changes in needs or requirements regarding log data, more patches, less hosts or more servers or more internal internet presence-- those would be flows.

Components of the Systems Model -2



Components of the Systems Model -2

○ **Converters** change inputs into outputs.   They usually represent the variables that initiate change. A converter might represent a sudden and drastic world event.

Ex. Leadership changes, business mergers, negative press, conflict, funding issues, acquisitions, new laws, new vulnerabilities or zero days, cyber attack

↱ **Connectors** link elements to other elements, representing assumptions about what depends on what.

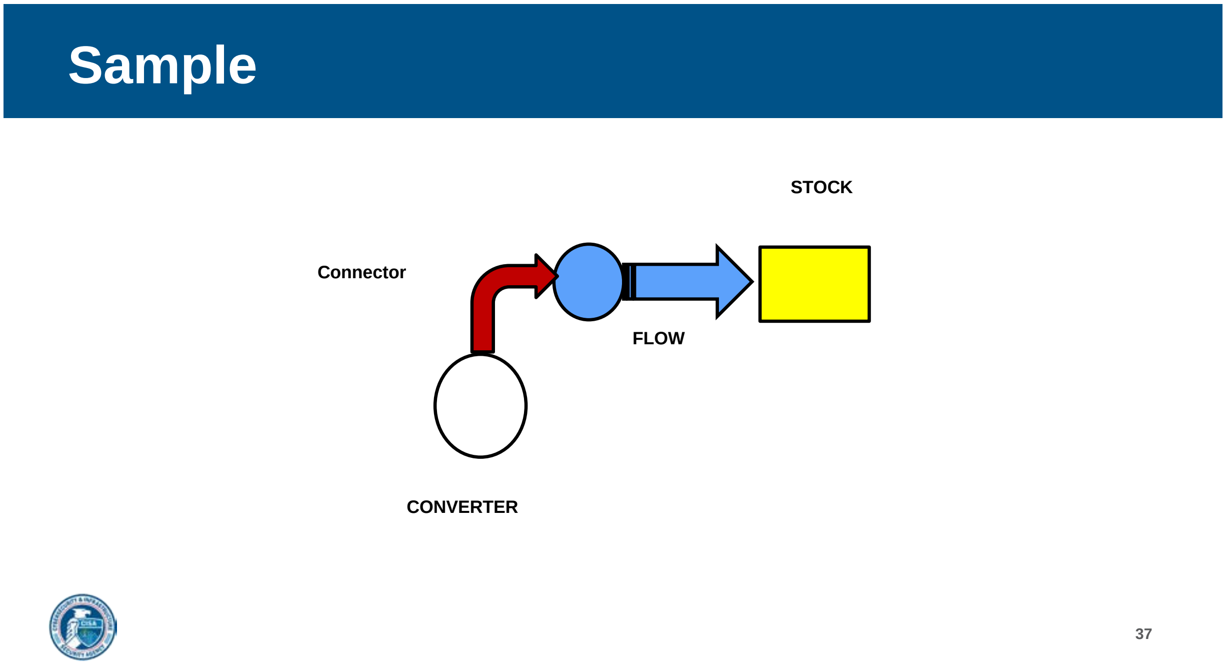
Dr. Rob Johnston. Analytical Culture in the US Intel Community. An Ethnographic Study. CIA. 2005 Washington D.C.

36

**036 Converters change inputs to outputs. They usually represent the variables that initiate a change. So a converter might represent a sudden or drastic world event, like a pandemic. Other examples could be leadership changes in your organization. That might lead to a whole new way of doing business, or a press report that your company is doing something nefarious. A war, a change in prices regarding what you're selling, a business merger, would be an example that something could initiate a change. A converter is, again, something that initiates change.

And connectors are things that link elements to other elements, representing assumptions about what depends on what.

Sample



Sample

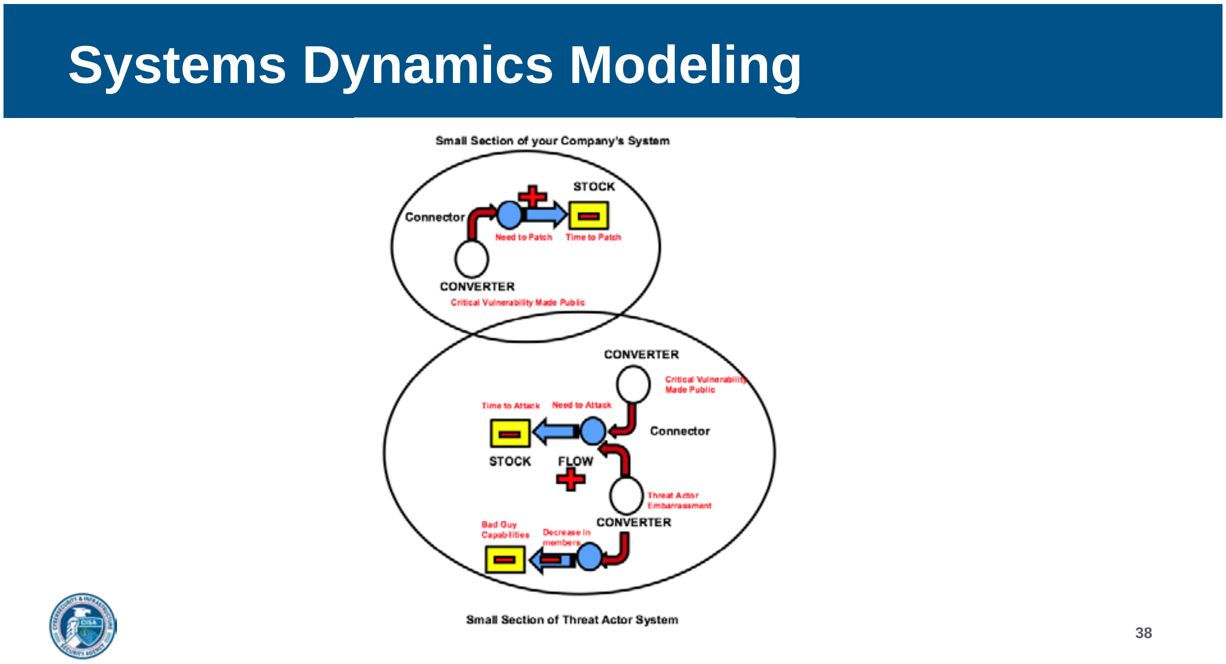
37

**037 So if you look at all of this together, it would look something like this, where you have these converters that are connected to flows that change the increase and decrease of a stock.

And Systems Dynamics Modeling could be useful because as a cyber intelligence analyst, you could outline your company as one system and one or two threat actors that you know based on intelligence and that is intent on attacking your organization or has already attacked your organization as a completely different system.

So if you were, for example, to put both of these into a larger system, your own organization and a threat actor, you could ostensibly be able to model changes over time when both systems are possibly vulnerable or in positions of strength.

Systems Dynamics Modeling



Systems Dynamics Modeling

Small Section of your Company's System
STOCK
Connector
Need to Patch
Time to Patch
CONVERTER
Critical Vulnerability Made Public
CONVERTER
Critical Vulnerability Made Public
Time to Attack
Need to Attack
Connector
STOCK
FLOW
Threat Actor Embarrassment
CONVERTER
Bad Guy Capabilities
Decrease in members
Small Section of Threat Actor System

38

**038 So I think there are programs that draw these out for you better than I can on PowerPoint-- this is me just playing around with shapes-- but I think you could probably get the picture here. But let's say you have over time classified intelligence that says a particular threat actor has been intent on targeting your agency or company, and then you get information about a new critical vulnerability that impacts operating systems your company uses. So for your company, the top circle, the converter is there is a new critical vulnerability that is out there. The flow is now you need to patch. Your need to patch has increased, which is the plus sign. The stock is your time to patch has decreased, the minus sign, because you know that this particular threat actor is now intent on attacking you and now may have a way in to your organization.

For the threat actor, the bottom circle, the converter is the same-- a critical vulnerability has been made public. The flow is a need to attack now has increased, a plus sign. The stock is a minus sign for the attacker as well. The time to attack has also decreased. So for converter, you could also, for example-- a converter in the example for this circle for the attacker might be something embarrassing has also happened to the threat actor organization. For example, maybe you have intelligence that said there was a major doxing event which led a connector to show a decrease in a flow of members for the threat actor group and a subsequent decrease in the stock of the threat actor's capabilities because some very skilled hackers left.

As a result, you might adjust your assessment on whether or not this particular threat actor does have the capabilities to target your organization. In any case, Systems

Dynamics Modeling from this particular perspective can give you a broader understanding of systems and might help you make more informed assessments of the likelihood of attack, or if there was an attack what would happen to your system then.

Notices

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM20-0262